APPENDIX A

Warfighter Information Network-Tactical

This appendix provides an overview of the primary equipment systems and information exchange processes found at various echelons corps and below (ECB) and is not intended as an all-inclusive description or identification of each. Refer to the appropriate systems' technical manuals for detailed information.

The warfighter information network-tactical (WIN-T) is the integration of emerging and existing command, control, communications, computer and intelligence (C4I) technologies and concepts designed to increase the security, capacity, and velocity of information distribution throughout the battlespace in order to gain information dominance. The maximization of secure information services will provide the warfighter with key enablers for each element of the Force XXI pattern of operations: project, protect, gain information dominance, shape the battlespace, decisive operations, and sustain operations.

The WIN-T serves to enhance maneuver force mobility by providing network security and interoperability support to the ABCS and its battlefield functional areas (BFAs). This concept of communication/information services will provide a force multiplier to the warfighter as current and future operations make greater demands on tactical voice, data, and multimedia signal support systems.

To provide warfighters with key decision-making information, the various information systems must be integrated into one homogeneous “system-of-systems” that encompasses the strategic, operational, and tactical levels as well as support of joint operations. Currently, the WIN-T information systems available to the ECB warfighter are global command and control system-Army (GCCS-A), standard Army management information systems (STAMIS), defense message system (DMS), and ABCS.

The GCCS-A supports joint and strategic planners of all the services with a common system to manage and execute crisis and contingency operations and provide a means to interface to Commanders-in-Chief (CINC), services/agencies C4I systems for peacetime deliberate

planning as well as crisis planning and execution. The GCCS-A is the realization of "C4I for the warrior" concept. The concept builds upon lessons learned from previous conflicts, operational requirements, and the effects of rapidly changing technology.

The warfighter requires a seamless information system, where boundaries between functions and sources are erased. The GCCS-A provides the seamless, integrated information to the warfighter when, where, and how it is needed. This enhances warfighter effectiveness by driving interoperability through the elimination of duplicated functionality and the convergence of joint warfighter doctrine via GCCS-A's encapsulation of common command, control and intelligence (C2I) methods. The GCCS-A uses the secret internet protocol network (SIPRNET) as its communications backbone.

The goals of the GCCS-A are:

- For all CINCs, provide one system that integrates across services and functions to provide the warfighter with a single picture of the battlespace.
- To migrate legacy applications to modern computing principles and technologies through the use of a COE.

To support these goals, the GCCS-A includes applications that provide efficient monitoring, planning, deployment, employment, and sustainment of military operations from the national command authority (NCA) to the commander, joint task force level.

The STAMIS is composed of separate logistical, medical, and personnel information management systems that provide a continuos flow of information from sustaining base through the tactical level. These systems are currently not seamlessly integrated but rather are sub-systems residing on separate computer platforms. To bridge this gap, the GCSS-Army initiative is proposed to fulfill the role of an integrated client/server system for all manning, arming, fixing, fueling, transporting, and sustaining support to the warfighter.

The DMS will be the single electronic messaging system for all DOD fixed, mobile, strategic, and tactical environments. The DMS will replace the automatic digital network (AUTODIN) and e-mail messaging systems used today to provide greater services and eliminate interoperability problems currently experienced.

The ABCS will be the ECB warfighters primary integrated information system to functionally link strategic, operational, and tactical headquarters and a more detailed discussion of its structure follows.

ARMY BATTLE COMMAND SYSTEMS (ABCS)

A-1. The ABCS supports leaders and planners at tactical to strategic level through an integrated digital information network designed to provide automated C2 and SA information through a seamless data architecture of existing and planned C2 systems. The ABCS includes the global command and control system-Army (GCCS-A), the Army tactical command and control system (ATCCS), and the Force XXI battle command-brigade and below (FBCB2) systems.

A-2. The GCCS-A supports Army strategic planners in the allocation, logistics support, and deployment of operational/tactical forces to the combatant commands in response to strategic planning and policy guidance provided by the NCA during crisis situations and operations from conventional conflict to stability and support operations (SASO).

A-3. The ATCCS integrates the five battlefield functional area disciplines: maneuver; fire support (FS); air defense (AD); combat service support (CSS); and intelligence. Each of these functional areas is supported by a control system designed to provide leaders and planners with information to effectively plan, coordinate, control, and direct the battle. These BFA control systems (BFACS) are oriented toward combat operations and provide the commanders and staffs at corps and below with situational information and decision support in executing operational/tactical battle.

A-4. The FBCB2 is a battlefield, battle command information support system supported by existing and emerging communications, sensors, and electrical power sources. The FBCB2 is both a system and a concept to be used by combat, combat support (CS), and CSS units across all BFA disciplines while performing operations at the tactical level. The FBCB2 includes both embedded battle command (EBC) software and Appliqué tactical computers. The EBC software is designed to run on the five BFACS workstations to provide a capability to share FBCB2 lower echelon SA with those BFACS. Messages are exchanged through message formatting and conversion capabilities of the COE common message processor (CMP).

ARMY TACTICAL COMMAND AND CONTROL SYSTEM

A-5. At echelons above company level, ATCCS provides additional C2 and SA information by providing commanders and staff synchronization tools in the exchange of information during

operations. The BFACS are linked through four communications systems: combat net radio (CNR), area common-user system (ACUS), Army data distribution system (ADDS), and broadcast systems (BDCST).

- **CNR.** Provides users with similar command or functional interests the ability to communicate using short-range, line-of-sight (LOS) radios (i.e., SINCGARS SIP); long-range, beyond-LOS radios such as improved high frequency radios (IHFR); and single-channel tactical satellite (TACSAT) transceivers. This communication means may be voice or data depending on the operational need.
- **ACUS.** Provides telephone, facsimile, and data transmission services from maneuver battalion through echelons-above-corps (EAC) to the sustaining base through gateways. At ECB, mobile subscriber equipment (MSE) transmits both circuit switched and packet switched data. At EAC, tri-service tactical communications (TRI-TAC) provides this same service. Currently, efforts are underway to modernize the ACUS to commercial, standards-based information system architecture to support the WIN-T. This effort is known as the ACUS modernization plan and the product will be the WIN-terrestrial transport wide area communications network that replaces the ACUS.
- **ADDS.** Includes the EPLRS VHSIC and joint tactical information distribution system (JTIDS)/multi-functional information distribution system (MIDS). Both systems optimize the use of data transmission and have no voice capability. It provides near real-time data between automated systems.
- **BDCST**. Provides technology similar to commercial television and radio stations, where transmit-only stations send information to many receive-only stations. The joint surveillance target attack radar system (JSTARS), tactical information broadcast service (TIBS), and global broadcast services (GBS) are examples.

Battlefield Functional Area

A-6. Within each BFA are C2 component systems tailored to support information flow, processing, and storage capabilities managed according to the needs of the BFA. The flow, processing, and storage of information among BFACS are then managed according to the needs of the force level commander. The combined arms team's commander and staff exercise force level control (FLC) by integrating and synchronizing the efforts of the BFAs to support the mission. This is accomplished by managing information from the BFAs and development of tactical plans and orders based on that information. The FLC functions by providing ATCCS support to the force commander and staff in their employment of the combined arms team.

A-7. The BFACS employed at ECB are maneuver control system (MCS), advanced field artillery tactical data system (AFATDS), all source analysis system-remote work station (ASAS-RWS), air and missile defense planning control system (ADPCMS), and combat service support control system (CSSCS). Command and control systems included in the ABCS configuration are FBCB2, aviation mission planning system (AMPS), combat terrain information systems (CTIS), integrated meteorological system (IMETS), and grenadier blue force reporting and tracking (BRAT) system.

Maneuver Control System

A-8. The MCS is the maneuver component of ATCCS. It is the primary information system supporting the commander and staff. The MCS provides the principal operational interface with necessary applications to access and manipulate the force level database to realize the FLC concept. There are a wide array of capabilities available, which make planning and executing a battle plan more efficient. Capabilities range from modifying UTOs to creating overlays. Commanders and staffs update the MCS database by entering readiness data, battle plans, and battle plan changes as they occur at each echelon.

A-9. The MCS consists of window and menu-based software allowing system operators to process, retrieve, store, and send information in textual or graphical form. Reports, OPORDs, overlays, UTOs, and messages are available to the user.

Advanced Field Artillery Tactical Data System

A-10. The AFATDS is an integrated fire support C2 system capable of processing fire missions and related information to coordinate and maximize all FS assets to include field artillery, mortars, attack helicopters, air support, naval gunfire, and offensive electronic warfare.

A-11. Fire missions are processed through the FS chain to the weapon system at the lowest echelon that can bring most effective fire upon the target after target attack criteria is satisfied. This distributed processing capability allows the maneuver commander to influence the battle by placing the right mix of firing platform and munitions on enemy targets based on the commander's guidance and priorities.

A-12. The integration of all FS systems through the distributed processing capabilities of AFATDS provides greater flexibility and mobility to FS units and allows greater management of critical resources. It provides current battlefield information, target analysis, unit status, and coordinates target damage assessment coordination and sensor operations.

Air and Missile Defense Planning and Control Systems (AMDPCS)

A-13. The AMDPCS system is an integrated system of weapons, sensors, and C2. It protects maneuver forces, critical CPs, CS and CSS elements from low-altitude air attack. It controls and integrates AD engagement operations and combined arms force operations for AD elements. To support engagement operations, the AMDPCS engagement operations (EO) system responds to air threats by integrating targeting functions, including sensor operations and AD weapons C2 functions. It acquires and tracks incoming air threats, identifies friendly and enemy aircraft, and automatically alerts forward AD weapons. The air and missile defense workstation (AMDWS) assists battle managers in planning, coordinating, synchronizing, directing, and controlling the counter-air fight. The AMDWS assists in developing and disseminating timely target data to all forward area air defense (FAAD) components. To support force operations, the AMDPCS system provides force level commanders with the information needed to integrate AD into the overall tactical plan.

All Source Analysis System-Remote Work Station (ASAS-RWS)

A-14. The ASAS-RWS is a functionally integrated intelligence support system. It manages sensors and other resources; collects, processes, and fuses intelligence data; stores, manipulates, and displays this data; and quickly disseminates information to the commander by providing a common picture of enemy activity.

A-15. The ASAS-RWS supports the commander's decision-making process 24 hours a day whether on the battlefield or in rear support areas. It prioritizes and manages collection assets; processes, receives, and correlates data from strategic and tactical sensors and other sources to produce ground battle situation displays. The system then disseminates intelligence information to assist the commander in refining that guidance, aids in target development, and provides recommendations.

Combat Service Support Control System

A-16. The CSSCS is the logistics component of ATCCS and provides critical, timely, integrated, and accurate automated logistical information. This system provides information on all classes of supply, maintenance, medical services, personnel, and movements to commanders and staffs. This information is consolidated and collated into situation reports and planning estimates for current and future operations.

A-17. The CSSCS provides a concise picture of unit requirements and support capabilities by collecting, processing, and displaying information on key items of supplies, and personnel that the commanders deem crucial to the success of an operation. Items tracked in CSSCS represent a small portion of the items managed by standard Army management information systems (STAMIS).

A-18. The CSSCS also supports the decision-making process with course of action (COA) analysis. Staffs can analyze up to three COAs for a 4-day period. Variables include combat intensity, combat posture, unit task organization, and miles traveled and geographical region.

A-19. The CSSCS maintains a database of unit personnel and equipment authorizations by source requirements code (SRC, similar to TOE) and unit and equipment planning factors. The CSSCS includes a database of equipment and personnel called a baseline resource item list (BRIL). The items that a commander identifies as critical to the operation can be selected from the BRIL to establish the commander's tracked item list (CTIL).

A-20. The commander will identify a CSSCS plans and operations officer who is responsible for developing and coordinating the plan to establish the CSSCS nodes and network. The CSSCS plans and operations officer functions are critical to the success of the CSSCS network and require substantial planning and preparation. The CSSCS plans and operations officer should be of sufficient rank and experience to influence subordinate and adjacent CSSCS nodes. The CSSCS plans and operations officer responsibilities include:

- Ensure that each echelon is resourced properly to operate CSSCS. This includes ensuring the unit has adequate communications to support CSSCS, trained operators, adequate power supply, and ancillary supplies such as paper and magnetic/optical media.
- Coordinates collection of information to build the CSSCS database. Quantities of supplies for units and supply points, personnel strengths numbers, task organization, support relationships, proposed data flow, and required and controlled supply rates.
- Ensures that CSSCS operations are integrated into all OPLANs, OPORDs, and annexes. This integration is critical to successful operations. The CSSCS operations must be included in logistics rehearsals. Continuity operations (CONOPS) must be outlined in applicable orders.
- Ensure that TSOPs contain current CSSCS operations information. The CSSCS operational aspects that are standardized across an organization must be included in unit SOPs. This facilitates hasty establishment of CSSCS operations in a combat environment.
- Coordinates training, maintenance, and troubleshooting of CSSCS.

A-21. Seven critical steps in establishing the CSSCS network and database are:

- Configure the unit task organization IAW the current OPORD.

- Develop data flow diagrams and build message handling tables IAW the diagrams.
- Develop the commander's tracked item list (CTIL).
- Establish status threshold percentages.
- Determine and set support to supported relationships.
- Establish reporting procedures and schedules for the command.
- Establish continuity operations pairing.

Army Airborne Command And Control System (A2C2S)

A-22. This is an UH-60 helicopter equipped with common networked computers, CNRs, HAVE QUICK UHF radios, SATCOM, HF radios, and a digital map flat panel display to provide commanders from corps to maneuver level a mobile C2 node for coordinating aviation support. It has the capability to communicate and exchange information with aviation, maneuver, intelligence, FS, close air support, and any other elements similarly equipped.

Aviation Mission Planning System

A-23. The AMPS is an automated aviation mission planning, rehearsal, and synchronization tool designed specifically for the aviation commander. There are two levels of AMPS; brigade/battalion and company. Each level provides the automated capability to conduct aviation missions. The brigade/battalion AMPS is hosted on the common hardware/software II (CHSII) platform. This consists of a tactical computer unit (TCU) with a removable hard disk drive, a CD-ROM drive, a magneto optical (MO) drive, a color monitor, and a character graphics printer. All of these components are ruggedized for field use. Additionally the AMPS has an internal -baud modem. Embedded within AMPS software is a modem applet allowing two AMPS to transfer data files over telephone lines. Longbow Apache and OH-58D Kiowa Warrior AMPS have a data transfer receptacle and data cartridge for loading/downloading mission data in the aircraft. The AMPS will be found in the maneuver brigade's aviation cell.

Improved Data Modem (IDM)

A-24. The IDM is a modem that passes targeting or SA information to and from airborne or ground platforms (digital and analog). The IDM replaces the airborne target handover system (ATHS) but retains backward compatibility with ATHS. It supports four links and one generic interface processor used for LINK/MESSAGE processing (link formats include TACFIRE and air force applications program development [AFAPD]). The IDM provides digital connectivity between Army, Air Force, and Marines providing C4I data exchange for attack and reconnaissance helicopters, TOCs, CAS aircraft, and near real-time intelligence assets. It is designed to be hardware and software expandable and flexible. The IDM is

used on the A2C2S, AH-64D, OH-58D Kiowa Warrior and in the aviation TOC (AVTOC). The Longbow Apache uses a software version that includes INC functions allowing for data exchange with other INCs. Variable message format (VMF) messages are not currently capable of being interchanged between the two versions. Limited radio assets on airborne platforms require operators to switch to a maneuver support net when providing CAS.

Integrated Meteorological System (IMETS)

A-25. The IMETS provides a tactical automated weather data system for receiving, processing, and disseminating information to provide timely weather environment effects, forecasts, and decision aids. The IMETS produces, displays, and disseminates weather forecasts and tactical decision aids that compare the impact of current, projected, or hypothesized weather conditions on friendly and enemy capabilities. The IMETS workstations are ATCCS common hardware and are interoperable with ASAS-RWS, DTSS, and other ATCCS BFAs over tactical and area communications.

Digital Topographic Support System/Quick Response Multicolor Printer (DTSS/QRMP)

A-26. The DTSS/QRMP is a mobile automated terrain analysis system supporting battlefield operations at division to echelons above corps. This system is located at the supporting engineer battalion TOC to provide digitized and hard copy maps, terrain studies, photography, climatic summaries, weather forecasts and reports, and other data sources. It provides a geographic information system to answer questions regarding terrain, mobility, bridges, and other geographic features using tables, maps, image files, and other products.

Battlefield Video Teleconferencing (BVTC)

A-27. The BVTC is a state-of-the-art, near full-motion interactive video teleconferencing system. The BVTC enhances coordination and provides an additional combat multiplier to the warfighter. Two areas that will see great enhancements by the use of BVTC are warfighter C2 and telemedicine.

A-28. The BVTC enhances C2 by allowing the warfighter to effectively disseminate orders, clearly stating his intent. He can conduct collaborative planning and whiteboard functions with subordinate commanders and key staff elements.

A-29. Medical units are supported by telemedicine from remote deployment areas, where deployed medical forces receive assistance from specialists at sustaining-base hospitals. Other applications exist at several regional medical centers (Tripler, Walter Reed and Landstuhl) to provide specialized diagnosis and care to remote medical facilities. Telemedicine will project the valuable expertise and skills of rear-based specialists to forward-deployed medics.

A-30. The BVTC components (cameras, monitors, computers, microphones, etc.) are user-owned and operated. The features and capabilities employed at each echelon or activity will be based on the requirements of that specific echelon or activity. The WIN-T architecture will provide the bandwidth and throughput required to support BVTC for both point-to-point and multi-point conferencing. The BVTC capability will be provided to users of the WIN-T with nominal impact on the remainder of the network.

A-31. Whiteboard application allows commanders and staffs to share and annotate documents, presentations, and graphics during a BVTC conference. Documents can be captured and graphics imported in the whiteboard and superimpose edit marks on the page. Editing is accomplished using markup tools in the whiteboard application.

ABCS COMMUNICATIONS AND NETWORKING

A-32. The physical configuration of command posts, the communications equipment available to support them, and the ABCS LAN infrastructure varies with the information flow requirements at each echelon. While these diversities exist, the foundation for communications and networking within all Force XXI tactical operations centers (TOC) remain relatively the same. The integration of C2 functions are achieved through the ATCCS that attempt to provide a set of shared common services. To fulfill this shared setting, a client-server architectural environment exists to integrate and allow interactive information processing. The client computer and associated software requests the service and the server and its associated software provide the service. This data information media exchange process is accomplished over a LAN or wide area network (WAN).

Distributed Computing Environment (DCE)

A-33. The DCE provides the means to maximize software components found on different workstations across the network. No one computer with all applicable software could effectively run all required operations at a speed usable by operators. A remote procedure call (RPC) allows a client and server to exchange information and the DCE environment provides security and synchronization services.

A-34. All workstations host a variety of client applications because each computer uses these to perform necessary services. Servers perform the dual role of ATCCS BFACS workstation and ATCCS server. A machine may thus act as a client in accomplishing one function but as a server in accomplishing another. The client applications are available to each workstation within a TOC with the majority of common services provided by a single workstation designated as the TOC server. Larger TOCs may have multiple TOC servers to ensure redundancy, even distribution of the server workload, and a capability to execute split/jump TOC operations.

A-35. The server database is automatically updated from its clients. This database is known as the joint common database (JCDB) or sometimes as the ABCS common database (ACDB) and contains all CSS, intelligence, air defense, fire support, maneuver, and network management information contained by each BFACS. When a BFACS receives information or performs some analysis, it stores that data in its resident JCDB. The servers then update other servers throughout the chain of command with any changes to the JCDB. This ensures that all unit databases remain current.

A-36. In an ATCCS client-server configuration, each server can have multiple clients connected to it in a LAN. When a user on a client machine executes a specific application, the client requests the data from the server to which it is connected (an RPC). The software operates exactly the same on either machine, and the user cannot tell on which machine the software is resident. The disadvantage in this configuration is that if the server fails or if the LAN is broken, the cell will only be able to perform the functions resident on the client until reconfigurations or repairs to the LAN are completed.

A-37. Through a process known as beaconing, the DCE, network, and system administration workloads can be minimized allowing greater automation of DCE and network configurations. This process also allows for unique cell set up and identification of DCE and network problems. Beacon provides reconnection of client BFACS temporarily disconnected from the cell LAN without having them reboot.

A-38. In addition to the TOC server, each TOC has a map server to provide digitized map products and data. Also found down to battalion level will be a global broadcast service (GBS) receive terminal and associated receive broadcast manager (RBM) that is a server that manages the receipt and distribution of data received over GBS.

A-39. The workstation designated as the TOC server provides several services. These include:

- EBC server - Identifies, parses, and makes available FBCB2 SA information to BFACS in a TOC.
- Communications server - Responsible for receiving, sending, storing, deleting, and forwarding messages. This server services e-mail messages using standard commercial messages and C2 messages in USMTF and JVMF formats.
- FTP server - Provides a means to transfer files in the TOC environment using standard networking protocol that allows point-to-point file transfers over the LAN or WAN, transfer of MS Word documents between and among BFACS, and SITMAP files between BFACS.

- Mail server - Manages mail message traffic and provides for translating and converting messages to allow exchange between systems.
- Network server - Provides various services to the BFACS to allow them to function as members of the network. Also, the network server is host to network management protocol services such as dynamic host configuration protocol (DHCP), lightweight directory access protocol (LDAP), domain name server (DNS), and command and control registry (C2R) services.

Local Area Network

A-40. A LAN is a group of computers and related equipment connected together using data cables for the purpose of sharing files and other resources between several users. The capability to have a wireless LAN exists in certain maneuver TOCs, however the majority of digitized TOCs will be the physical cable plant type. The type of data cable used is a coaxial cable or fiber optic cable providing connectivity for inter-LAN connections. Unshielded twisted pair cable with is used for intra-LAN connections. Fiber optic cable is used to connect a LAN when distances between LAN vehicles are such that the total LAN cable length will be greater than 600 feet, or if greater durability and data capacity is required.

A-41. An ABCS LAN consists of multiple BFACS sharing the same LAN at a CP. The tactical packet network (TPN) also known as the MSE packet switch network, or MPN serves as the communication link for the WAN which connects the various ABCS LANs across the battlefield (See Figure A-1). The primary assets used for TPN communications include the node center (NC), small extension nodes (SEN), large extension nodes (LEN), and the system control center (SCC). These assets form the backbone of the tactical network linking the ATCCS LANs. Introduction of technologies such as asynchronous transfer mode (ATM) switching, high speed multiplexer circuit card (HSMUX), high capacity line-of-sight (HCLOS) radios, high capacity trunk radios (HCTR), near-term data radio (NTDR), satellites, and range extension terminals all assist in bandwidth management and improved quality of service. A more thorough explanation of these can be found in FM 11-55, MSE Operations.

A-42. While the CSSCS, AFATDS, AMDPCS, and ASAS-RWS BFACS may also operate their own internal LANs for stovepipe communications, the ABCS LAN is the primary communications path for passing digital information horizontally between BFAs. Each ABCS LAN is a high-speed, short distance network for computer-to-computer communications. It has an effective transfer rate of approximately 10 Mbs per second and is implemented with the Institute of Electrical and Electronics Engineers (IEEE) base LAN standards and a bus topology. Channel access is through carrier sense, multiple access/collision detection (CSMA/CD).

Packet protocol is transmission control protocol/internet protocol (TCP/IP). The system is similar to the commercial ethernet standard and the terms ethernet, thin LAN, and IEEE base2 are often used interchangeably.

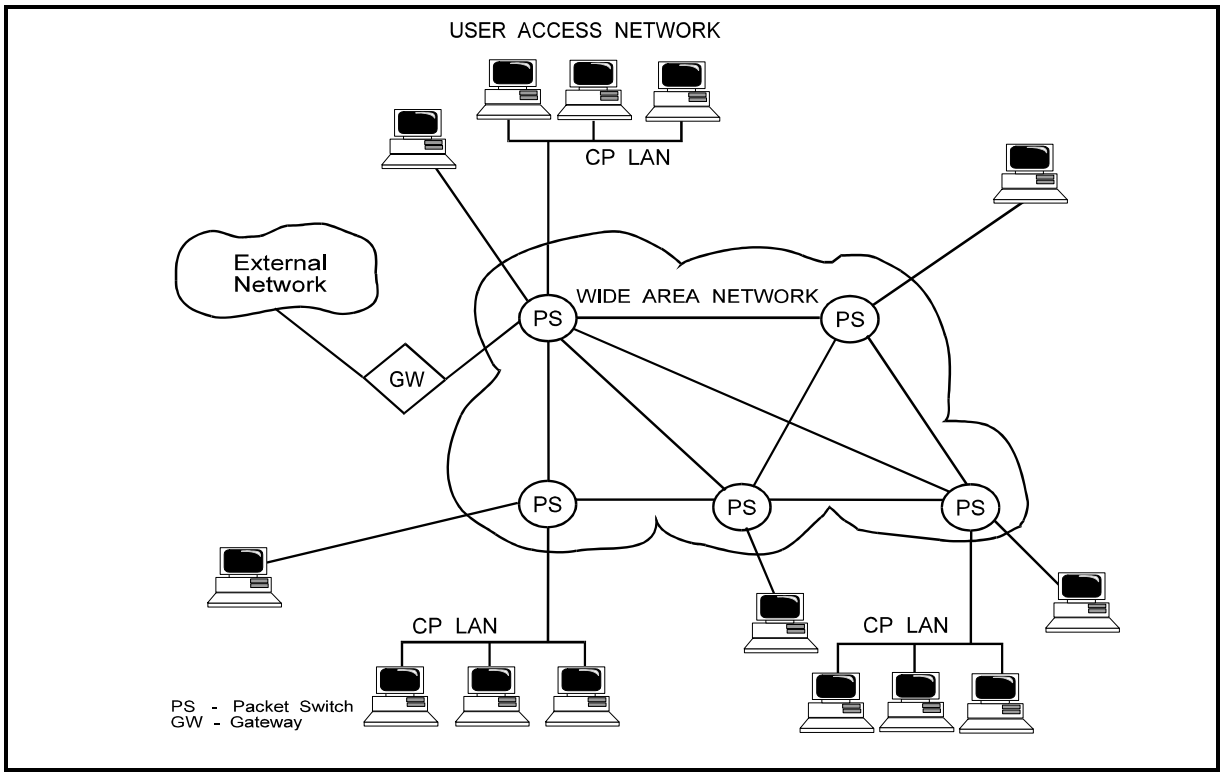

Figure A-1. Simplified TPN Architecture

A-43. A TOC LAN will generally consist of two segments, as depicted by Figure A-2, called LAN-A (edge component or intra-vehicle LAN) and LAN-B (core component or inter-vehicle LAN). A third LAN-C exists for the FSE to extend the AFATDS workstation into the TOC SICPS. The LAN-A connects all peripherals (workstations, printers, etc.) that are found within a single vehicle, tent or standardized integrated command post system. The LAN-B allows for interconnection among all TOC LAN-A segments to provide information exchange across the TOC.

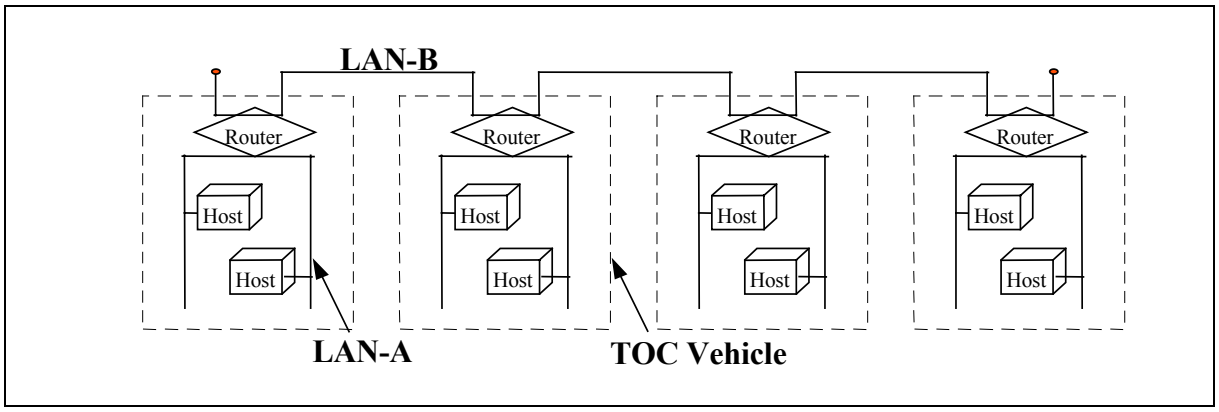

Figure A-2. Example TOC LAN Connectivity

A-44. The LAN-A is implemented by using a standard twisted pair connection, ethernet hubs, or routers/switches. Where LAN-A components access LAN-B, a router is used to simplify IP address management and internet work forwarding decisions. This also enhances efficient use of available bandwidth within a LAN. A router determines if a message is delivered to the local TOC or forwarded to another TOC (see Figure A-3).

A-45. The LAN-A exists within the larger core TOC LAN (LAN-B). There may be multiple LAN-A components within a LAN-B network and the connections will vary according to the echelon involved and the complexity and bandwidth requirements of the overall TOC.

A-46. The LAN-B is the connectivity among all ABCS TOC components normally part of one of the LAN-A components such as a single vehicle or SCIPS. To maximize available bandwidth LAN-B networks use routers and Ethernet switches.

A-47. An ABCS BN TOC contains a stand-alone router or a router embedded in an Ethernet switch (a router-switch) in each vehicle. At brigade and division TOCs, an Ethernet switch or a router-switch is found in each vehicle. The router-switch combines both functions of a router and a switch. Ethernet switches make local forwarding decisions to devices within the LAN (see Figures A-4, & A-5).

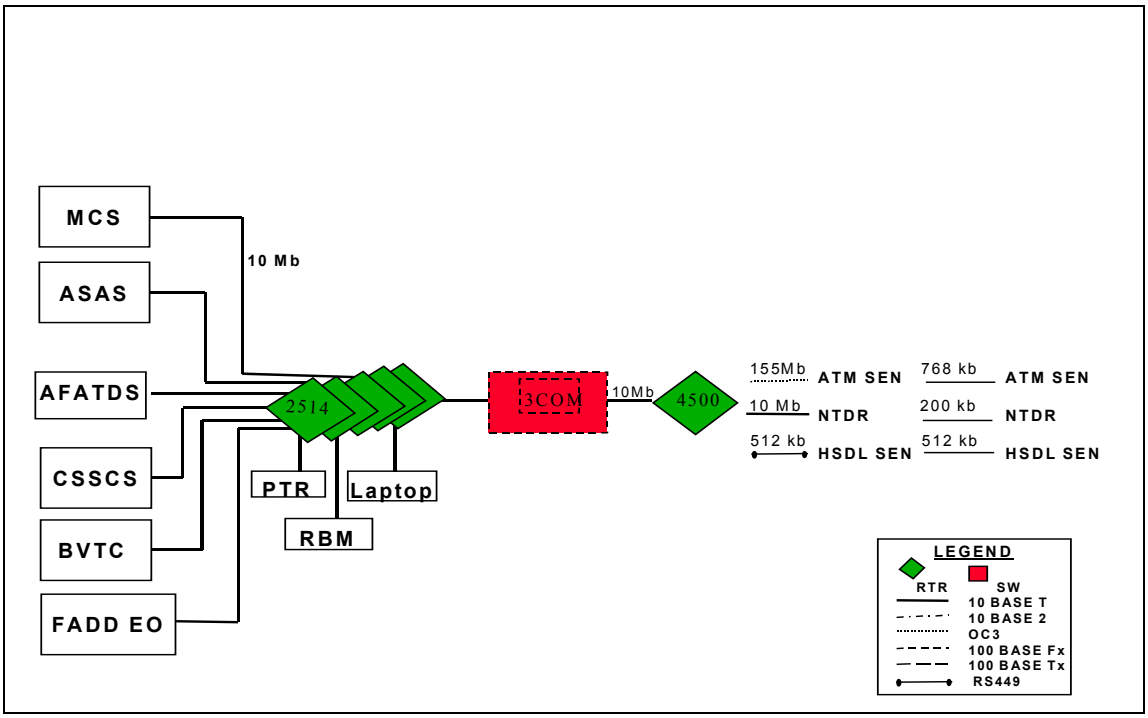

Figure A-3. Router-based TOC Architecture

A-48. Digitized TOCs use a minimum of two core routers embedded in a central ethernet switch connected in a star configuration to one of the core routers to create a multi-star network configuration. This configuration reduces initial configuration complexity due to less router usage, and therefore, it improves performance.

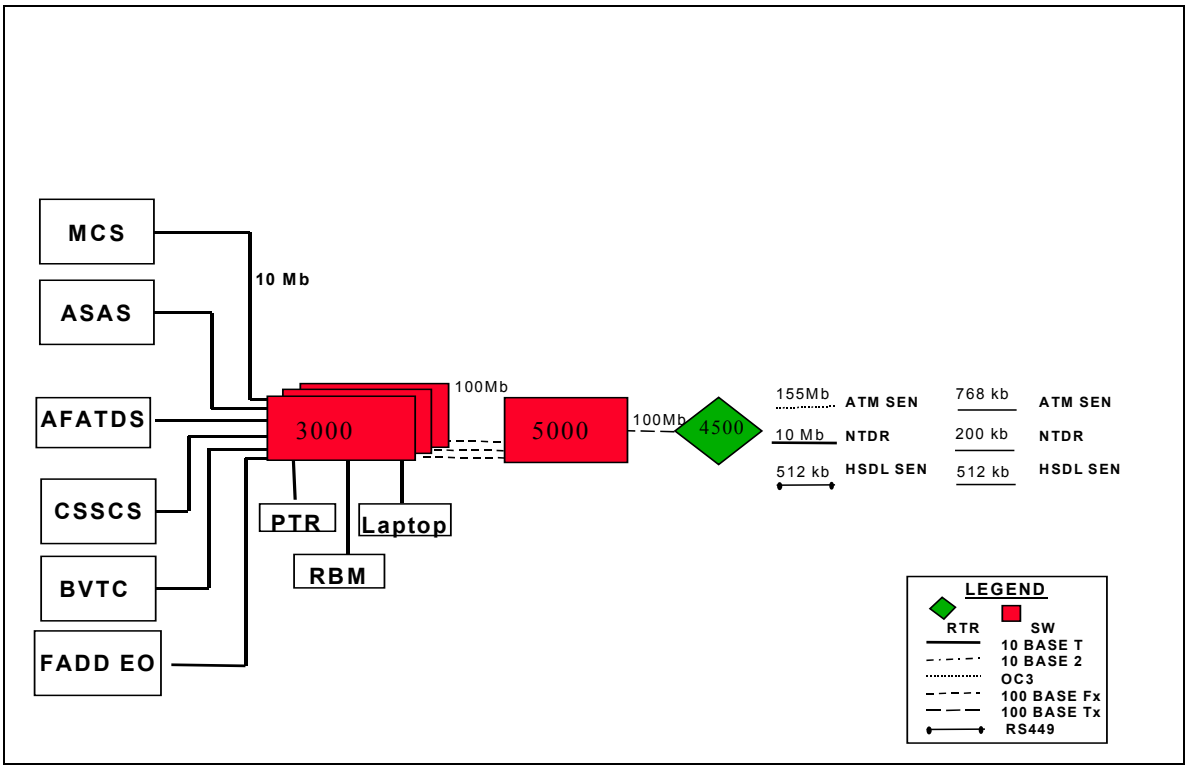

Figure A-4. Switched-based TOC Architecture

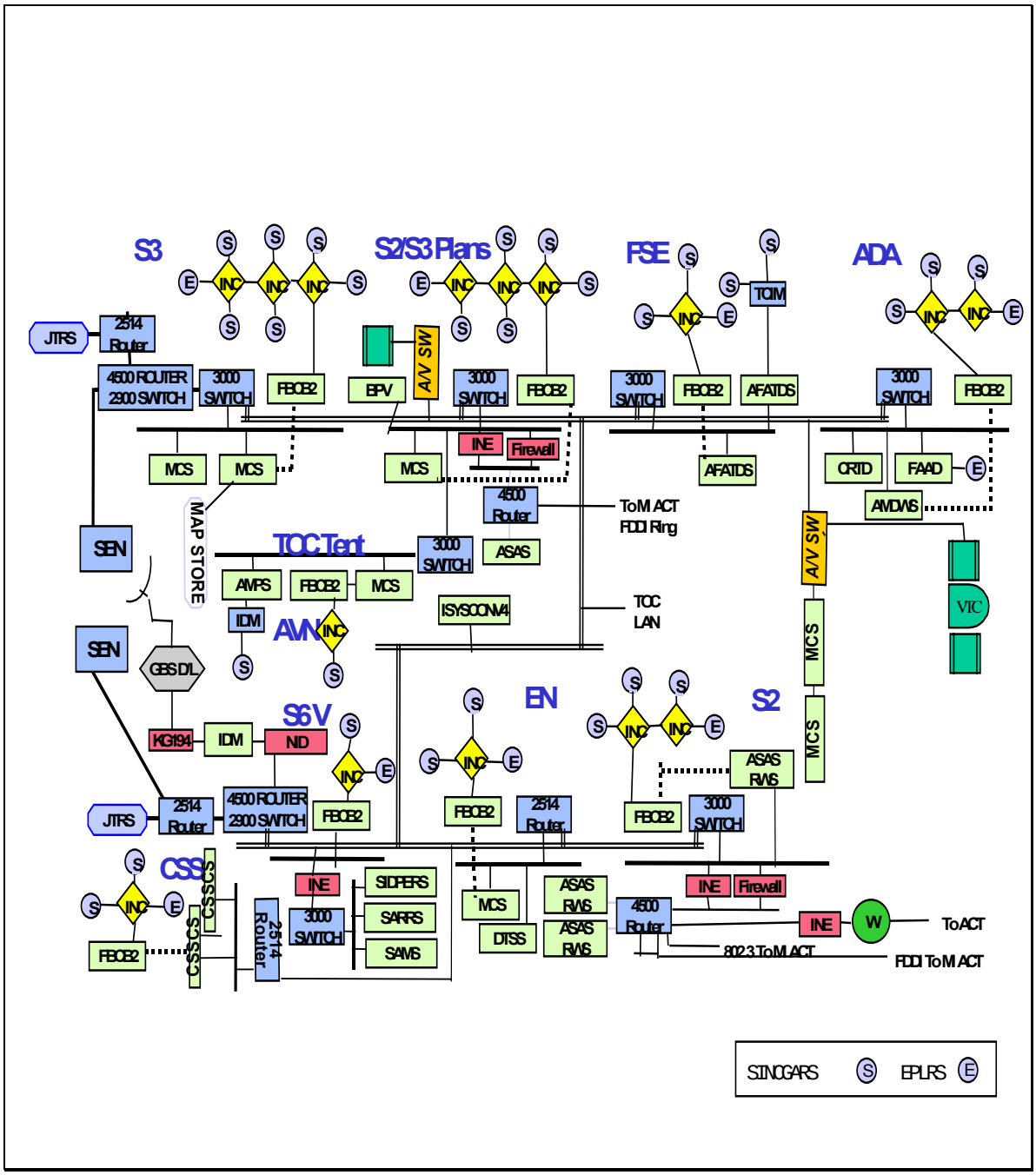

Figure A-5. Example Brigade TOC LAN

Wide Area Network

A-49. A WAN is similar to the LAN but covers a larger distance and allows LANs to communicate to higher, lower, and adjacent units. It is a network of networks that is constructed from a number of LANs connected to each other and to radio networks such as CNR or MSE. Because of the limitations of a network constructed with coaxial cable, a WAN uses a combination of the MPN and radio networks to distribute the data where necessary through the system.

A-50. The gateway switch at the supporting signal brigade/battalion is responsible for managing the WAN. The WAN consists of several networks designed to allow wider access to C2 information. These networks are MSE, GBS, and NTDR.

A-51. The MSE network is a common-user, switched communications system of linked-switched nodes that form a grid of voice and data communications on an automatic, fixed-directory basis using flood search routing techniques. Flood search techniques initiate each call over multiple routes and establishes the connection over the optimum route based on current traffic within the network. A thorough explanation of MSE can be found in FM 11-55, MSE Operations.

A-52. The GBS network is a joint program that features commercial, direct broadcast technology to deliver high volume, bandwidth intensive products such as video, data, imagery, weather, maps and theater and national level intelligence to joint forces. The GBS system consists of three major segments: broadcast, terminal and space.

A-53. The broadcast segments are composed of the satellite broadcast manager (SBM) and receive broadcast manager (RBM). The terminal segment is comprised of the primary injection points (PIPs), theater injection point (TIP), fixed and mobile ground receive terminals (GRTs), shipboard receive terminals (SRTs), and airborne receive terminals (ARTs). The PIP is a fixed earth station that sends data streams from the SBM to a specific satellite where it is relayed to GRTs in Theater. The TIP is a smaller, transportable version of the SBM and PIP. The TIP can be found at a designated tactical TOC such as division or corps main. The TIP can allow large theater generated information products such as UAV and satellite imagery, operation orders, and overlays to be transmitted to theater users. The space segment is composed of satellites in geosynchronous orbit.

A-54. The NTDR network consists of brigade and below mobile packet radios that provide a high data rate capability for increased throughput. The NTDR is an interim program to create a data backbone for platoon to brigade for Force XXI. It is the TOC-to-TOC radio for maneuver echelons transmitting data files greater in size than what EPLRS can handle or when MSE is not available.

There are two NTDRs per multiple vehicle ABCS TOCs, and one NTDR for single vehicle ABCS TOCs. MSE and other WIN-T assets provide WAN trunking for higher echelon TOCs not equipped with NTDRs.

TACTICAL INTERNET (TI) OVERVIEW AND CONCEPT

A-55. The tactical internet (TI) is the term for both the physical communications network that provides the general-purpose data backbone and also the overall concept of an integrated battlespace automated infrastructure. The "tactical internet" is named as such because of the wide and intentional similarities to the commercial internet.

A-56. The TI forms two distinct information exchange layers depicted in Figure A-6 called the upper and lower TI. The upper TI layer is composed of MSE, multi-channel satellite systems, and other WIN-T systems. The lower TI is the communications support system for units found at brigade and below and is composed of the FBCB2 computers and software, EPLRS, and SINCGARS SIP radios networked together using routers and commercial and military protocols.

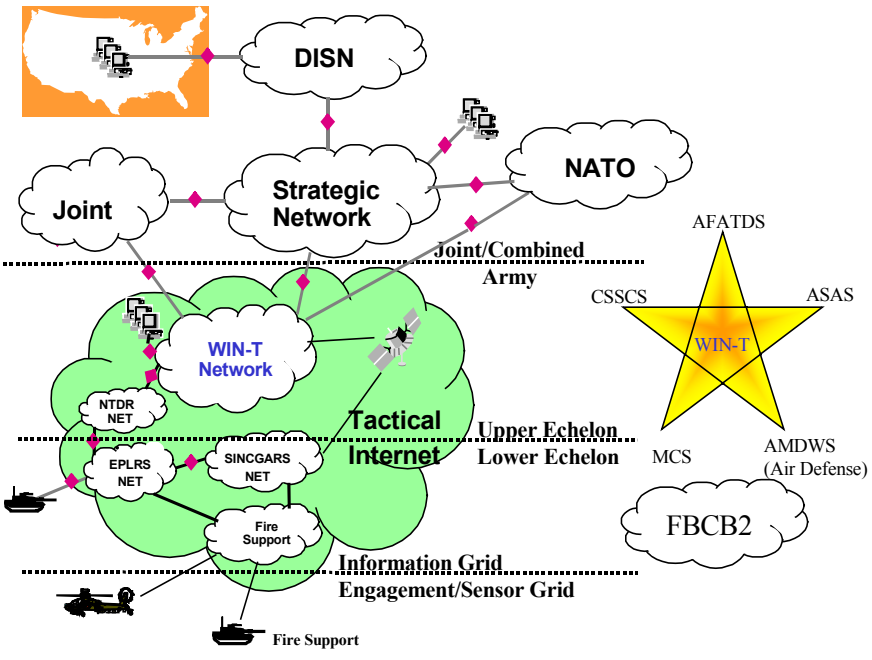

Figure A-6. WIN-T Conceptualization

A-57. The upper TI constitutes all available in-theater communications assets that allow corps, division, brigade, and separate maneuver battalions to exchange information. Components of the upper TI or WIN-T consist of improved MSE TPN assemblages containing ATM technologies, HCLOS, HCTR, NTDR, and multi-channel satellite systems such as secure mobile anti-jam reliable tactical terminal (SMART-T) and SHF Tri-band advanced range extension terminal (STAR-T). These satellite terminals help extend the MSE range between node centers and ECB command posts and provide split-based operations capabilities.

A-58. The lower TI layer key communication systems being employed are the:

- The FBCB2 host computers (includes Appliqué and in selected platforms embedded battle command [EBC] software).
- Enhanced position location reporting system (EPLRS) very high speed integrated circuit (VHSIC).
- Near-term digital radio (NTDR).
- Single-channel ground and airborne radio system (SINCGARS) System improvement program (SIP) with internet controller (INC).
- The MSE TPN.

A-59. The lower TI architecture consists of two substructures that support command and control (C2) data and voice, and provide situational understanding information (friendly and enemy locations). These substructures operate simultaneously, are transparent to the user, and are governed by the types of service requested by the host (See Figures A-7 & A-8, C2 & SA architectures).

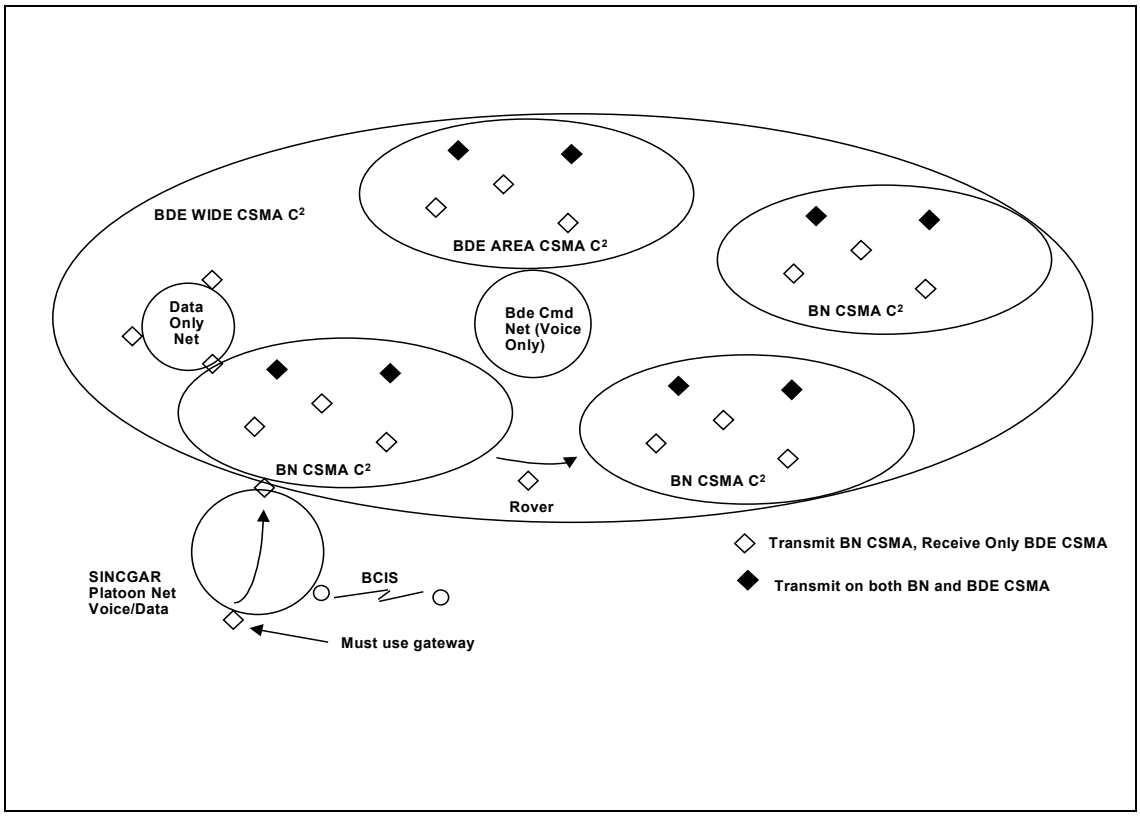

Figure A-7. Example TI C2 Architecture

A-60. Designed as the primary communications architecture supporting the warfighter at brigade and below, the network allows sharing of C2 data by users which results in near real-time SA and thereby improves force C2 for enhanced lethality, OPTEMPO, and survivability.

A-61. The TI is designed to electronically link all users so critical C2 and SA information is available to make tactical decisions. Planners and operators communicating within the TI must understand their particular role and that of their operational platform. Turning off radios, FBCB2, or improper initialization of equipment will impact the overall functionality of the TI. Operating within the TI carries with it an increased operator responsibility to ensure proper start-up and sustainment procedures are accomplished and a fundamental understanding of how the TI functions.

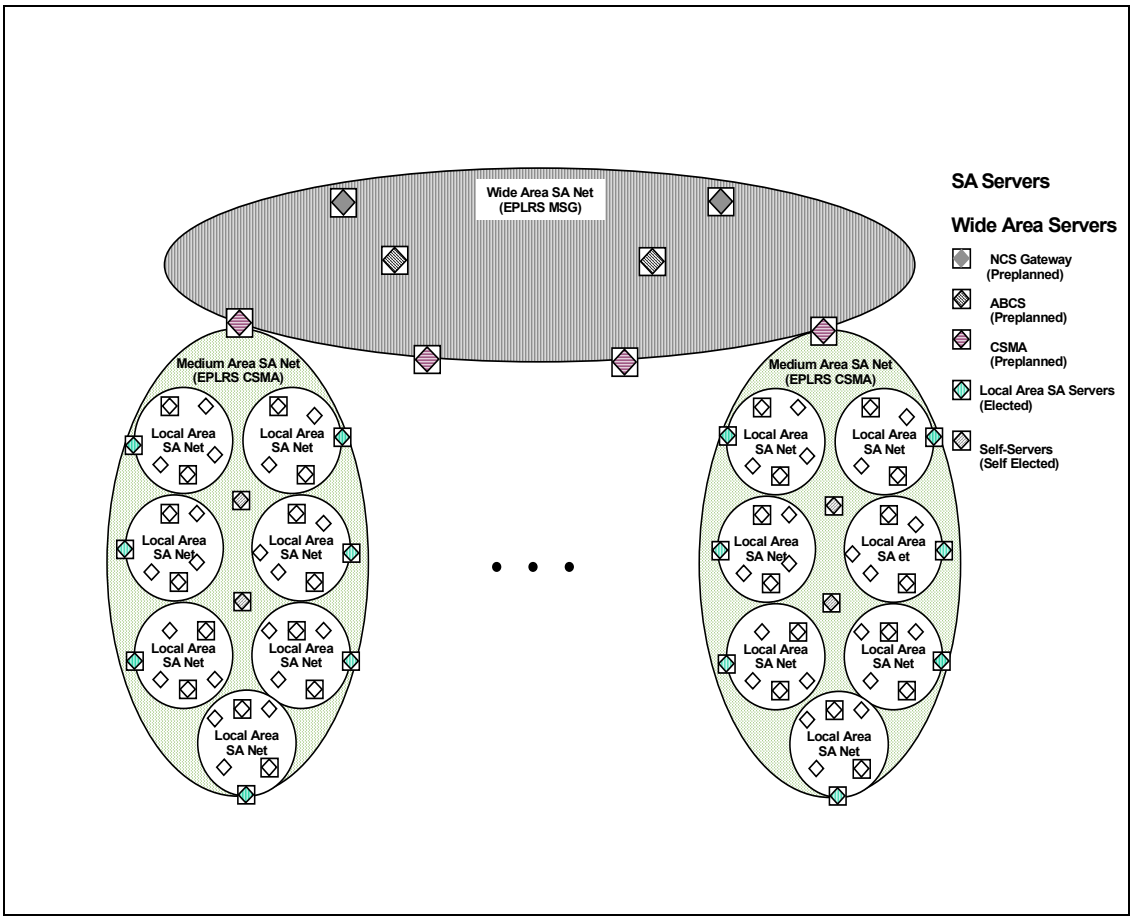

Figure A-8. Example TI SA Architecture

A-62. The C2 sub-architecture employs the use of EPLRS VHSIC full-duplex need lines for primary transmission of data; secondary means is SINCGARS SIP. Command and control data is defined as anything not classified as SA data. This data includes operational overlays, orders, reports, and free text messages formatted in FBCB2 to allow operators to send C2 information in the form of joint variable message format (JVMF) messages through an interface connection of FBCB2, SINCGARS SIP with INC, EPLRS VHSIC, and PLGR. Two types of delivery messaging methods are employed within the lower TI. These methods are uni-cast and multi-cast messaging.

A-63. Uni-cast messages are transmitted to a single destination using transmission control protocol/internet protocol (TCP/IP). The TCP/IP provides more reliability by using sequence numbers to coordinate which data has been transmitted and received. This type of transmission is more reliable, however it requires greater bandwidth overhead because it sends out a separate message to each addressee. The uni-cast method of transmission is used for C2 messages that exceed 576 bytes in size. Multi-cast messages

are used to deliver data to multiple destinations simultaneously. It is used for messages less than 576 bytes and is transmitted using user datagram protocol/internet protocol (UDP/IP). The UDP/IP is less reliable than TCP/IP, however it uses less bandwidth overhead than TCP/IP.

A-64. Multi-cast transmission conserves network bandwidth since a single message is sent and delivered to multiple addresses. If a multi-cast message is greater than 576 bytes, the user is sent a warning message and an option to send the message uni-cast. Mandating a maximum message size is to limit the chance of lost messages. Hosts are generally members of multi-cast groups that are identified as a dynamically determined group of IP hosts, such as a platoon or battalion, identified by a single IP multicast address. Any host or member may join or leave a multi-cast group at any time and may be participants of more than one group. One does not have to be part of a multi-cast group in order to send messages to members in the group.

A-65. Operators can set their FBCB2 to specified settings relative to time, motion, and battlespace as well as set their send settings to include precedence, retries, acknowledgment, and addressee display. Command and control information is transmitted, transparently to the operator, in accordance with available transmission capacity and was not designed for speed of service due to this unpredictable time required to send traffic. Therefore, it has no guaranteed speed of service as SA information has precedence within the TI as it travels through the routers and gateways.

A-66. The INC router determines which transmission means to send the messages based upon these priority filters, the transmission device available, and the RFC-1256+ protocol found in SINCGARS SIP only equipped units. The RFC-1256+ protocol allows each INC to select its own exit gateway. The gateway will be selected based on the highest preference level. Each INC router will periodically advertise its preference level along with its IP address. An EPLRS INC has the highest ranking preference values.

A-67. Additional routing protocols found within the lower TI include internet group management protocol (IGMP) used for IP hosts and IGMP+, which is used for both IP hosts and IP routers like those associated with SINCGARS SIP only equipped platforms. Additionally, internet control message protocol (ICMP) and address resolution protocol (ARP) are used. The IGMP/IGMP+ protocols are used by host computers and gateway routers to communicate to their routers about their interest in participating in a specific multi-cast group. The ICMP Network layer internet protocol reports errors and provides other information relevant to IP packet processing. The ARP is a protocol that translates an IP address to a physical machine address (MAC) that is recognized in the local network. For uni-cast messages, an ARP request message is

broadcast over the media by the interested host or router and is received by all stations. Stations recognize the IP address and reply by sending an ARP response. The local router for the host being requested responds or acts as a "proxy" for that host with the MAC address and a switched virtual circuit is created to transmit the information. Once the information is sent and a designated inactive period occurs, the circuit is deactivated.

A-68. The SA information primarily enables friendly forces to identify other friendly units and avoid fratricide. Situational understanding provided includes all friendly unit positions and known enemy positions from all relevant sources. Each FBCB2 reports its position over the TI to a designated SA server that disseminates the information based on filter settings and the SA sub-architecture. This process occurs automatically with minimal operator intervention once settings are established. Friendly locations are built from individual platform reports. Enemy locations are added from intelligence sources at brigade level and broadcast back down. The TI provides an intra-ABCS interoperability path at brigade and below. The FBCB2 system exchanges information with the higher level components of the ABCS in selected platforms such as the BCV, C2V, and A2C2S. This path allows the sharing of digitized data by commanders, staffs, units, and soldiers/weapon platforms resulting in near real-time SA and improved C2.

A-69. Because of the size of the TI to be deployed, it is necessary to split it into multiple autonomous systems (AS). These AS are a grouping of equipment that comprise a single net management domain (i.e., brigade/battalion areas).

A-70. Situational understanding is disseminated throughout the TI by a combination of SA servers broadcasting position reports. These SA servers may be local area, medium area, or wide area SA servers and are pre-defined according to the unit task organization (UTO), dynamic server selection process, client registration, and are usually equipped with EPLRS VHSIC. Local SA net servers process external SA data and local FBCB2 generated SA data onto local SINCGARS nets and send local FBCB2 data onto EPLRS CSMA need lines. Local area net (SINCGARS) members participate in automatically and dynamically selecting the most capable local SA server based upon an eligibility ranking scheme which includes equipment rank – platform communications equipment and their status; platform rank – vehicle type; and role code – hierarchical position within the unit. The best or most capable or highest-ranking FBCB2 platform selects itself as the local area SA server based upon each platform’s assessment of its condition using the eligibility criteria. If unable to register onto the SINCGARS SA net after a designated time and if the next hierarchy net is an EPLRS CSMA, the platform becomes a self-server. Only EPLRS VHSIC equipped platforms may be self-servers. This ensures flexibility of any platform, with the exception of SINCGARS only ones, to become the local SA server. This also

prevents lone platforms from becoming isolated from SA updates. The SA software in each FBCB2 host continually ensures a SA server is identified by continually updating each host's communication status, automatic sever selection, client registration and maintaining the active client list (ACL).

A-71. The ACL (a list of the clients who have access to the server's functions) is adjusted as clients de-register and/or areas-of-responsibility change due to battle-rhythm and attrition. If the local area SA server does not hear from the client over a period of 20 minutes or 3 client report times, whichever is greater, the client is dropped from the ACL. Clients consider themselves de-registered if not on an ACL or if they do not hear from the local area SA server over 3 report times but not to exceed 2 minutes. A local area SA server will relinquish local area SA net support to higher-ranking FBCB2 platforms. Clients will de-register from lower ranking local area SA server(s) if they appear on two or more ACLs.

A-72. Local area SA servers equipped with EPLRS VHSIC are best for allowing position reports to gain access to CSMA need lines. There is a CSMA need line established for each battalion and brigade area. All EPLRS VHSIC equipped platforms within a battalion or brigade area will listen on the CSMA need line. Each EPLRS VHSIC SA server will transmit the positions of all units for which it is responsible via the CSMA need lines to all other EPLRS VHSIC equipped platforms within the CSMA need line area-of-responsibility.

A-73. To disseminate SA data between CSMA areas, a multiple source group (MSG) need line is used. All EPLRS VHSIC radios in the battlefield can listen on the MSG. A few EPLRS VHSIC radios are designated as MSG transmitters in pre-operational planning. A primary and secondary wide area SA server is designated and the secondary takes over when it no longer hears SA data from the primary. It relinquishes its role when the primary returns.

A-74. The SINCGARS SIP radio is responsible for sending and receiving voice, SA, and C2 data for those platforms not equipped with EPLRS VHSIC radios. Interfacing with a PLGR and FBCB2 computer, SA information is broadcast to all SINCGARS SIP net members and the SA data is displayed on FBCB2 screens. The INC interprets the information from the FBCB2 and SINCGARS SIP and sends new position data to the nearest EPLRS VHSIC local area SA server and then to the CSMA need line thereby updating all members of a particular net.

A-75. SINCGARS SIP radios use SA agents that are activated by the FBCB2 computer when it sends its local INC a message to a special UDP port. With SA agents, the source INC strips off the UDP/IP headers of the SA messages before sending them to the EPLRS VHSIC CSMA or MSG. The destination INC replaces the header with a "dummy" header prior to forwarding it to the FBCB2 computer. The SA agents are applied to SA data transmitted over

SIP networks. Separate queues for SA and C2 data are established (known as "SA Up" "SA down", or "SA other"). This improves completion rates of C2 data over SIP networks.

TACTICAL INTERNET NETWORK PLANNING AND MANAGEMENT

RESPONSIBILITIES

A-76. The signal officer (G/S6) is the coordinating staff officer responsible for planning, coordinating, and managing the communications assets of the maneuver force including the TI. To accomplish this mission, the G/S6 and his staff must understand all phases of the mission, the commander's intent and the scheme of maneuver. The G/S6 is responsible for coordinating with the maneuver force G/S3 to determine the location of signal support nodes and C2 platforms during each phase of the operation and for coordinating additional communication support from the next higher supporting signal echelon. This support may include MSE and EPLRS systems, FM and HF frequencies, tactical satellite assets, and COMSEC keys and hardware. The S6 exercises operational control of all communications assets OPCON to the brigade.

PLANNING AND MANAGEMENT FUNCTIONS

A-77. The TI requires thorough planning and network management. The integrated system control (ISYSCON) suite of hardware and software, when fully functional, is the FBCB2 equipped task force's interface and management platform to the TI. Additionally, the brigade task force uses other systems to plan and manage the TI; they are network control station-EPLRS (NCS-E), FBCB2 or commercial computers configured for network management to plan and manage the TI. Network management requires four basic activities:

- **Planning.** The TI must be carefully planned to support specific mission requirements. The two most important steps in the planning phase are to:
  - Fully understand the mission, commander's intent, and scheme of maneuver.
  - Fully understand the characteristics, capabilities, and mission of the individual components of the TI.
- **Initialization.** The components of the TI must be initialized to a known state before the network can be used to pass SA data. Each system's technical manual contains procedures to place the individual equipment into operation. The TI quick reference guide (QRG) contains equipment initialization requirements and procedures demonstrated to work best.
- **Monitoring**. Once the network is operational, it must be monitored so problems within the network can be identified and corrective action taken.
- **Reconfiguration**: Elements of the TI may move or change status. The network manager has the ability to change the current configuration to support continuous, seamless communications.

PLANNING AND MANAGEMENT CONSIDERATIONS

A-78. Planning and management considerations the G/S6 needs to account for and operational users and planners at all levels should be aware of are:

- **Understanding the operational intent.** The G/S6 must understand the mission and operational intent. He must take an active part in developing the scheme of maneuver and the synchronization matrix for the FBCB2 equipped task force during all phases of the operation. This will ensure he plans for all contingencies and positions communications assets to support current and future operations.
- **MSE connectivity.** The digitized task force has the same level of connectivity to the MSE ACUS network as the non-digitized task force. The CSG S6 must coordinate with the G6/corps signal brigade to plan for the positioning of LOS systems and SENs to provide continuous access to the voice and TPN capabilities provided by MSE. See FM 11-43, The Signal Leaders Guide, for detailed information on planning and controlling MSE networks.
- **EPLRS networks and need lines.** The EPLRS network is the primary, general-purpose data traffic backbone from brigade to lower echelons. The basis for EPLRS radio connectivity is the EPLRS need line. Each need line defines the operational relationship between the source and destination EPLRS units, without specifying which additional EPLRS units are part of the connection. The type of transmitted data, the mode of operation, and the data rate effects the planning distance between individual EPLRS units and the number of “hops” or relays that can be included in an EPLRS link. Accurate planning and network configuration is critical to provide proper area coverage within the battlespace. See FM 24-41, TTP for EPLRS, for planning and controlling EPLRS networks.
- **NTDR networks**. The NTDR networks provide a wideband data path between major C2 nodes at CSG and battalion level. Accurate network configuration is essential to provide reliable vertical and horizontal data links between these nodes.
- **SINCGARS SIP networks.** The SINCGARS SIP is used in both the data and voice communications modes. However, when the net is used for voice traffic, data traffic is delayed. Radio net discipline is critical for effective use of this information media. Unit SOPs must define the triggers that cause a user or unit to switch from data to voice communications modes of operation.
- **IP Addresses and Plain Language Naming Conventions.** To have an effective Tactical Internet three functions must

occur in the planning process; addressing, naming, and routing schemes must be developed.

A-79. Additional information on network planning and management can be found in FM 24-32, Tactics, Techniques, and Procedures For The Tactical Internet at Brigade and Below, chapters 11, 12, and 13, the tactical internet naming convention document, and in appropriate technical manuals.

ADDRESSING AND NAMING CONVENTIONS

A-80. A standard Class B IP addressing scheme is used for hosts of the TI. Eventually, the goal is a classless inter-domain routing (CIDR) schema of addressing. Address assignments are determined for each device associated with the host's system. That is the INC, SINCGARS SIP, ELPRS, and FBCB2 will each have an address for routing of information. Essentially, each active data port will be assigned a unique IP address. Assignment of IP addresses will be based upon the network to which they communicate. Each IP network address may be formatted as network, sub-network, and host fields so that multiple hosts and sub-networks can be aggregated and advertised in routing updates.

A-81. Each of the individual addresses will form a unique identification for the given platform. This unique identification includes its IP address and an established FBCB2 host name or functional designator (e.g., "user role@hostname"). These are designated by the role of the user of the system and not by individuals. The host file contains the name and address of all the hosts within its organization. Reconstitution/reorganization of a unit requires re-initialization to load new host files containing the changes to UTO.

A-82. As individuals or users change due to battlefield or scheduled attrition, the role remains the same on the platform FBCB2 host without having to change configurations due to personnel change. It is only when the user changes FBCB2 host that changes are required to ensure accurate message routing. An example would be the commander having to use an FBCB2 other than his to send and receive messages. The commander would have to re-initialize that FBCB2 as performing the role of commander in order to obtain messages.

A-83. Name services conform to architecture that:

- Assigns entire CSG as single domain.
- Assigns a hostname.
- Assigns IP address of each host present in host file.
- Domains correspond to a specific numeric. (e.g., PL-3OF66.TFXXI.C3.ARMY.MIL)

A-84. See FM 24-32, Appendix B, and Tactical Internet Naming Convention, for additional details on the TI naming convention.

Crew Assignment Sheet

A-85. Each platform in the unit has a crew assignment sheet that graphically depicts all TI components, cabling, NET IDs and EPLRS need lines corresponding to the platform. The operator uses the crew assignment sheet, in combination with the QRG, to verify proper SINCGARS SIP NET IDs, EPLRS logical channel numbers (LCN) for need lines and unique EPLRS radio set identifier (RSID), and role names. Using the crew assignment sheet helps ensure each platform is correctly configured to communicate within the TI (See Figure A-9).

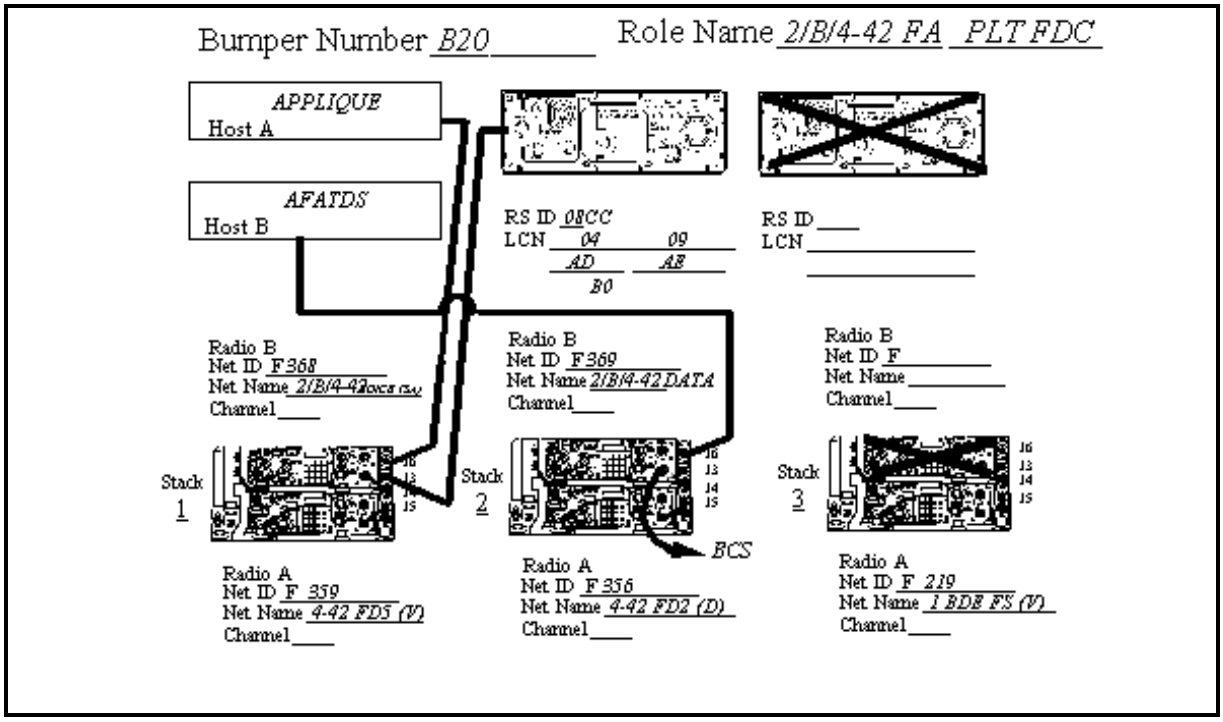

Figure A-9. Example Crew Assignment Sheet

Tactical Internet Quick Reference Guide

A-86. This document establishes the procedures to correctly initialize the primary components of the TI at the maneuver level based on approved techniques. It contains step-by-step instructions for operators to place the FBCB2, BCIS, EPLRS VHSIC, PLGR, PND, and SINCGARS SIP components into operation either separately or in multiple configurations, specific troubleshooting guides, crew assignment sheet, wiring and cabling

diagrams, and significant lessons learned as pointers to successfully operate within the TI.

TACTICAL INTERNET SYSTEMS

A-87. Within the TI are an assortment of digital systems designed to provide the commander and soldiers of all units of the brigade task force and below C2 and SA information. Each echelon of the task force will be comprised of that digital equipment essential for effective C2 and battlefield SA tailored to the operational requirement and particular role of platforms belonging to the unit.

SINGLE CHANNEL GROUND/AIRBORNE RADIO SYSTEM-SYSTEM IMPROVEMENT PROGRAM (SINCGARS SIP), RT-1523C/D

A-88. The SINCGARS SIP communications system replaces the RT-1523 through RT-1523B manpack radio and AM-7239 through AM-7239B vehicular adapter. The planning range of the SINCGARS SIP with AM-7239C/D and AM-7238 RF power amplifier is dependent upon the configuration, power out put, and data mode. Information regarding this can be found in FM 6-24.32 (24-32), Chapter 5 and TM 11-5820-890-10-8, Appendix F.

A-89. The SINCGARS SIP features, with a GPS device interface, embedded GPS position reporting in all voice and enhanced data mode (EDM) data messages to provide reporting of friendly force position in support of SA. The SINCGARS SIP uses the internet controller (INC) to provide packet radio relay nodes across the battlefield for horizontal and vertical integration of C2 data. It is designed to provide voice and data communications capability at all levels. It is the primary path for data transmission at the company, platoon, and squad/team level. The SINCGARS SIP with INC consists of the following major components:

- **Receiver-Transmitter, Radio RT-1523C/D**. The RT-1523C/D is common to all of the SINCGARS radio configurations. User controls and displays are on the radio front panel. Electrical connectors permit interfacing to audio and data devices, and to the other components of the radio configuration. This radio supports digital data communications with data rates of 600, 1200, 2400, 4800, 9600 and 1600 bits per second.
- **Amplifier-Adapter, Vehicular AM-7239C/D**. The AM-7239C/D vehicular amplifier-adapter (VAA) is used in conjunction with the MT-6352 mounting base for vehicular radio installations. The VAA fits on top of the mounting base and is secured by thumbscrews. The VAA contains mechanical and electrical provisions for mounting one or two SINCGARS SIP radios and one AM-7238 RF power amplifier. Provides packet communications through the internet controller card (INC). Routes signal through the mounting base for the vehicular intercom system and provide

connectors for user data terminal (UDT) interfaces to the INC. Provides an internet access point that connects VHF radio nets with ATCCS/FBCB2 external data systems and the MSE/ACUS voice/data backbone switching network. Provides an interface and distribution of external GPS signals to as many as four RTs. Provides asynchronous RS-232 and MIL-STD-188-114 interfaces.

- **Internet Controller**. The INC is the forward area Internet router responsible for routing data between two or more communications networks. The INC is mounted within the AM-7239C/D and provides a programmable interface for protocol conversion between BFAs to support a seamless architecture between BFAs. The INC provides the interface point with VHF radios, EPLRS, user data terminal (UDT) devices, MSE circuit switch or packet switch, and other INCs.

A-90. The SINCGARS SIP is employed in C2 and combat platforms at all levels. See Chapter 5, FM 6-24.32 (24-32) and TM 11-5820-890-10-8 for additional details on the SINCGARS SIP.

Enhanced Position Locating and Reporting System Very High Speed Integrated Circuit (EPLRS VHSIC), AN/VSQ-2 (V)

A-91. The EPLRS VHSIC radio set (AN/VSQ-2 (V)) is a state-of-the-art line-of-site (LOS) radio operating in the 420 - 450 MHz UHF frequency band. It provides secure, jam-resistant digital communications and accurate position location capabilities for the user. The EPLRS VHSIC uses time division multiplexing access (TMDA). Its use of frequency hopping (512 times per second), spread spectrum technology (eight frequencies between 420 Mhz and 450 Mhz), embedded COMSEC module (KIV-14), and adjustable power output provides secure communications with a low probability of intercept and detection. It has built-in-test (BIT) functions that are activated at power turn on. The EPLRS VHSIC uses an omni-directional dipole antenna capable of covering the 420-450 Mhz frequency ranges. The average distance between radios is 3 KM to 10 KM depending on power out settings and terrain. The EPLRS VHSIC provides retransmission functions that are transparent to the user. The maximum distance the EPLRS VHSIC can cover is based on 3 KM to 10-KM distance between each radio and the maximum number of relays in the link. Each radio can handle up to 30 Need lines. The maximum number of need lines available is dependent on bits per second required for each need line.

A-92. The EPLRS VHSIC is employed in the C2V, BCV, A2C2S, and TOC/TAC platforms at the CSG and battalion level. It is employed in the combat platforms of the commander, executive officer, first sergeant, platoon leaders, and platoon sergeants at the

company and platoon level. The EPLRS VHSIC is used as alternate data communications link (host-to-host) between C2 platforms at the brigade and battalion level. It is the primary data communications link between battalion C2 platforms and company/platoon combat platforms. The EPLRS VHSIC can be employed in RETRANS platforms and configured to provide retransmission capability.

A-93. The EPLRS VHSIC network is planned and configured using the net control station-EPLRS (NCS-E). The NCS-E is organic to the division signal battalion, and OPCON to the brigade. Network planners need the following information from the user to plan the network and radio configuration:

- Required speed of service.
- Maximum number messages the user will be transmitting during the users peak hours.
- Average message size (bits per message).
- Required bits-per-second (if known).

A-94. The S6, in coordination with the ADSO/G6 and signal battalion SYSCON, will plan the EPLRS VHSIC network using the NCS-E. The NCS-E sends network configuration data to each individual radio using remote file transfer procedures.

A-95. See FM 6-24.32 (24-32), Chapter 3, FM 6-02.41 (24-41), and TM 11-5825-283-10 for further details on the EPLRS VHSIC.

FBCB2 SUITE OF COMPUTERS

A-96. FBCB2 computing hardware are a mix of commercial, ruggedized, and militarized computers, system software, installation kits, application software, and integrated CSS support installed in vehicles and issued to individual soldiers. FBCB2 provides SA and C2 capabilities to all echelons of the task force through several input devices such as GPS, BCIS, SINCGARS SIP, and EPLRS VHSIC. The FBCB2 software users manual (SUM) contains additional information on and use of FBCB2 in the TI.

FBCB2 V1

A-97. This is a commercial off-the-shelf Intel 80486 DX4, 75 Mhz processor with an 80487 numeric co-processor. It has 16 Mbs expandable to 24 Mbs of RAM and an internal hard disk with 500 Mbs of storage and an internal diskette drive. It has an internal display on a flip-up lid of the note book computer. It has a 256-color liquid crystal display (LCD) and a diagonal measurement of 9.5 inches.

FBCB2 V2

A-98. This is a ruggedized version of an Intel Pentium P54C, 90 Mhz processor. It has a minimum of 16 Mbs expandable to 128 Mbs of RAM, an internal hard disk with a minimum of 500 Mbs of storage. It interfaces to external VGA, serial input/output (I/O) ports, parallel I/O, Ethernet, small computer system interface-2 (SCSI-2), and external diskette drive. It has an external video monitor with a diagonal measurement of 10.4 inches.

FBCB2 V3

A-99. This is a militarized version of an Intel 486 DX4, 100 Mhz processor. It has a minimum of 16 Mbs expandable to 64 Mbs of RAM, a removable hard disk drive with a minimum of 1.05 Gbs of storage. It has serial interfaces to external VGA monitor, serial I/O ports, parallel I/O, Ethernet, SCSI-2, and external diskette drive. It has an external color monitor with a diagonal measurement of 10.4 inches.

POSITION/NAVIGATION DEVICE (PND)

A-100. The position/navigation device is a computer that features an Intel 80486 DX33 processor. It has a minimum of 16 Mbs of RAM and an internal hard disk with a minimum of 170 Mbs of storage on a rotating hard disk unit. The PND interfaces to serial I/O RS-232 port (COM 1) dual-channel modem port, PCMCIA card, a GPS receiver antenna; dual-channel tactical modem and external power access port. The PND is designed to support vehicles not equipped with one of the other FBCB2 devices. The PND has a functional GPS card internal to the computer rather than relying on an external PLGR GPS receiver. The PND has a colorized LCD with internal display measuring 7 inches diagonally. It has a touch screen capability allowing the soldier to select “soft push buttons” from the FBCB2 display screen with a finger or with a stylus.

PRECISION LIGHTWEIGHT GLOBAL POSITION RECEIVER (PLGR), AN/PSN-11

A-101. This is a hand held, self-contained, multi-channel receiver capable of receiving the precise positioning signal (PPS) and tracking up to 5 satellites. It operates on battery or external power. It provides position coordinate, time, and velocity information. It can be operated hand held or vehicular, aircraft, or facility mounted.

A-102. The PLGR receives spread spectrum radio frequency (RF) signals from satellites orbiting the earth. These signals contain a unique code sequence and a navigational data message the PLGR uses to calculate a 3-D position by measuring the time the signal takes to travel from the satellite to the PLGR. This travel time is multiplied by the speed of light to determine the distance to the satellite. Repeating this calculation to four satellites provides the PLGR operator a 3-D position. Velocity is determined by measuring the rate of change of the signals. Time data is part of

the navigational message component of the RF signal, derived from an atomic clock onboard each satellite.

A-103. Up to 99 data way points may be entered, stored and selected as a destination. A route may consist of up to 9 legs (10 way points) linked together, start to end or end to start. Fifty-one map datum sets are available. Maps have two associated datum, horizontal and vertical (altitude). See TM 11-5825-291-13, Operations and Maintenance Manual for Satellite Signals Navigation Set, AN/PSN-11 for additional details on the PLGR.

COMMERCIAL OFF-THE-SHELF (COTS) ROUTERS & SWITCHES

TACTICAL MULTINET GATEWAY (TMG)

A-104. The TMG is a commercial-off-the-shelf (COTS) modular access router (CISCO 4000 series) with the primary function of routing data between two or more communications networks. The TMG uses the TCP/IP protocol suite to provide routing based on IP addressing. The TMG supports interconnection between tactical packet network (TPN), SINCGARS SIP w/INC, ATCCS LAN, EPLRS VHSIC and the LAN Router. The TMG has the following features:

- Four Ethernet (IEEE 802.3) ports.
- Four serial ports.
- 40 MHz Motorola 68EC030 processor.
- 4MB flash EPROM memory and 4M DRAM allowing fast, reliable software updates.
- CISCO internetwork operating system (IOS) supporting TCP/IP, Novell IPX, and AppleTalk routing for bandwidth control and security.
- Data compression ratio of 4:1 for WAN speeds up to 128 Kbps.

A-105. The network planner using CISCO point and click configuration software generates the mission-specific configuration database. This software is resident on the network management tool (NMT [B2]) found in the ISYSCON (V) 4 and NTDR. The configuration database is generated at the NMT (B2) prior to deployment and downloaded to a 486-laptop computer belonging to the unit's organizational maintenance personnel (31U). Changes to the mission-specific database will be generated using the NMT (B2) and distributed using the procedures described below.

A-106. The using unit's 31U personnel are equipped with 486 laptop computers. They will receive (download) the mission-specific configuration database generated by the network planner using NMT (B2). The 31U will then upload the mission database into each TMG prior to deployment. Changes to the mission-specific database will be provided to the unit using the same

procedures (NMT [B2] generated and downloaded to the 31U on his 486 laptop. The 31U then up-loads the database to each TMG).

LOCAL AREA NETWORK ROUTER

A-107. The LAN Router is a commercial-off-the-shelf fixed configuration router (CISCO 2500 series) with the primary function of linking Ethernet LANs to wide-area networks and is employed in the BCV and C2 platforms at all echelons. The LAN Router uses the TCP/IP protocol suite to provide routing based on IP addressing. The LAN Router supports interconnection between TPN, SINCGARS SIP w/INC, ATCCS LAN, and EPLRS VHSIC. The LAN Router has the following features:

- Two ethernet (IEEE 802.3) ports.
- Two serial ports.
- 20 MHz Motorola 68030 processor.
- 4MB flash EPROM memory and 4M DRAM allowing fast, reliable software updates.
- CISCO internetwork operating system (IOS) supporting TCP/IP, Novell IPX, and AppleTalk routing for bandwidth control and security.
- Data compression ratio of 4:1 for WAN speeds up to 128 Kbps.

A-108. The LAN Router mission-specific configuration database is generated and distributed in a like manner as mentioned with the TMG. See FM 24-32, Chapter 1, 9, and 10 for additional information on the TMG and LAN Router.

COMMERCIAL ETHERNET SWITCHES

A-109. Several series versions of CISCO ethernet switches can be found within various echelons of Force XXI CPs. Among these are the CISCO 3000, 4000, and 5000 series of high-performance, stackable switching platforms. The stackable architecture of these switches allows for greater flexibility and easier network and configuration management.

A-110. Switches are data-link layer devices that enable multiple physical LAN segments to be interconnected into a single larger network. Switches forward and flood traffic based on MAC addresses. Because switching is performed in hardware instead of in software, as a bridge would, it is significantly faster. Switches use either store-and-forward switching or cut-through switching when forwarding traffic. Many types of switches exist, including ATM switches, LAN switches, and various types of WAN switches.

A-111. The LAN switches are used to interconnect multiple LAN segments. LAN switching provides dedicated, collision-free communication between network devices, with support for multiple

simultaneous conversations. LAN switches are designed to switch data frames at high speeds.

NETWORK MANAGEMENT TOOL (BRIGADE AND BELOW (NMT [B2])

A-112. The NMT (B2) is network management software hosted inside the ISYSCON (V4) and NTDR on a SunSPARC20 workstation. The NMT (B2) in the brigade is designed, when it becomes fully functional, to provide the primary means of supporting the TI with planning, initialization, and network monitoring and control. Network data can be viewed as network log, tree, or diagram menus.

A-113. Nominally, one NMT (B2) per AS is responsible for monitoring the performance of the communications within that AS and initiating corrective action when necessary. There is a NMT (B2) for the brigade rear area, each maneuver battalion task force AS, and any support battalion AS that is established.

A-114. The NMT (B2) directly manages only the routers in the AS (INCs, TMGs, LAN routers), not the FBCB2 hosts. It monitors EPLRS VHSIC systems via the NCS-E, monitors FBCB2 locations, allows modification to existing network configuration and development of future configurations.

NEAR-TERM DIGITAL RADIO (NTDR)

A-115. The NTDR is a brigade and below mobile packet radio used to interconnect ABCS and is employed in the C2V, BCV, A2C2S, and TOC/TAC platforms. It is used as the primary data and imagery communications link (host-to-host) between C2 platforms at the brigade and battalion level and up to 400 radios may be employed to serve a nominal brigade area of operations. In the host-to-host mode, each NTDR provides a relay function that is transparent to the user and has network management capability through NMT. The NTDR can be employed in RETRANS platforms and configured to provide dedicated retransmission capability. It operates in the 225-450 Mhz frequency band, has a point-to-point data rate of 288 Kbps and range of 12.5 kilometers at 20 watts of output power. This radio is providing a technical baseline for development of a multi-band, multi-mode digital radio system which is currently being termed the joint tactical radio (JTR).

A-116. When establishing the individual NTDR nets, it is important to ensure that the nets are interconnected at several points. This will allow users with net access in one net to send messages into another net. The interconnection points will typically be in the CSG and battalion TOCs. This allows messages to be automatically tunneled through the ethernet LAN connections within the TOCs from one net to the other net.

SPITFIRE, AN/PSC-5

A-117. The SPITFIRE SATCOM terminal will provide command and control for the division and corps warfighter nets, support SOF C2, and SASO. This Single-channel UHF SATCOM will replace the AN/PSC-7 (MST-20plus), AN/PSC-3, AN/VSC-7, AN/MRC-140, and AN/PSC-10 terminals currently used for the warfighter nets.

A-118. The terminal will utilize demand assigned multiple access (DAMA) and advanced narrow band digital voice terminal (ANDVT) techniques. It has embedded COMSEC and TRANSEC capabilities for data, voice, and order wire communications. It supports data rates of 75-4800 bps (5 kHz) and 16 Kbps (25 kHz), weighs 11.6 lbs., operates in the military UHF Band of 225-400 MHz, and is deployable in man pack, vehicular, and aerial operations.

A-119. Spitfire has the ability to transfer data from units such as the brigade recon using the advanced data controller for TCP/IP (ADC/IP) which connects to the ethernet port of the INC. The ADC/IP acts as a bridge between two networks using UHF SATCOM.

SECURE MOBILE ANTI-JAM RELIABLE TACTICAL TERMINAL (SMART-T)

A-120. The SMART-T is a HMMWV mounted MILSTAR SATCOM terminal that will provide multi-channel range extension for the WIN at division and corps. It provides low probability of intercept and detection, built-in transmission security with over-the-air rekeying, and a capability to interface and control certain aspects of the satellite such as resource control and antenna pointing. It supports 16 Kbps up to 1024 Kbps and 1544 Kbps commercial rate.

A-121. The SMART-T uses extremely high frequency (EHF) spectrum and will replace the multi-channel ground mobile forces (GMF) SATCOM terminals at corps and below. It is interoperable with MILSTAR, FLTSAT EHF packages, and EHF Packages on UHF Follow-On (UFO) satellites.

SHF TRI-BAND ADVANCED RANGE EXTENSION TERMINAL (STAR-T)

A-122. The STAR-T is a HMMWV mounted multi-channel TACSAT terminal. It has tri-band capability in the SHF range and operates over commercial and military SHF satellites. There are two versions of the STAR-T; standard and switch. The both versions consist of communications equipment, power generation, and an antenna system. The switch version has embedded automatic switching equipment.

A-123. The STAR-T provides communications connectivity for split-based operations between the theater and the sustaining base. Theater TACSAT companies deploy up to 20 standard STAR-Ts to provide range extension links between selected EAC node switches and/or key headquarters. Links are provided to the supported corps/deployed units for entry into the EAC switched networks. Links are also provided to other services, joint/allied

headquarters, staging bases and other locations depending on deployment requirements.

SINGLE CHANNEL ANTI-JAM MANPACK TERMINAL (SCAMP)

A-124. The SCAMP is a man-packable terminal designed to interface with the MILSTAR low data rate (LDR) payload (it can also operate over EHF packages on FLTSAT and UFO/E). The terminal has anti-jam, intercept, COMSEC, and exploit capabilities and low probability of detection, interception, and exploitation capabilities to reduce the effectiveness of radio electronic combat and to reduce the possibility of destruction. It operates in point-to-point and broadcast modes and provides voice and data service at a maximum data rate of 2.4 Kbps.

A-125. The terminal will provide range extension for CNR as required by ALO and special operations. The SCAMP (Block I) will be used for critical command and control (voice/data) communications between headquarters elements and their major subordinate elements.

INFORMATION AND NETWORK SECURITY

SYSTEM FUNCTIONALITY DESCRIPTION

A-126. Army digitization efforts are intended to field a wide range of embedded and stand-alone end-user computers, connected by a universal TCP/IP data network. That network will consist of heterogeneous data-capable radio networks (e.g., SINCGARS, EPLRS, NTDR, MSE) and wire communication links (e.g., local area networks), and these links will be connected and supported by a network infrastructure of specialized computers (e.g., switches, routers, name servers, security servers). Although manufacturers design systems with security in mind, and highly skilled personnel follow appropriate procedures, the Army cannot field a "bullet-proof" network. Consequently, it is necessary to maintain the ability to do real-time security management and intrusion detection as part of routine operations and to take appropriate reactive measures when problems occur. The information systems protection concept, for ABCS, envisions real-time security management as a component of network and system management.

A-127. Several security tools used to implement information and network security are listed as follows:

- Internal and external firewalls.
- Internal and external network intrusion detection systems (NIDS).
- In-line network encryptor (INE).
- Communications security (COMSEC).
- Security guards.

- DCE security services.
- Host based C2 protect tools.
- TCP wrappers.
- Security profile inspector (SPI).
- SWATCH.
- Secure shell.
- Password checker.
- Anti-virus McAfee's virus scan for Solaris.
- Purge.

A-128. It should be noted that external firewalls and NIDS refer to devices that are on the perimeter of the WIN-T and MSE data networks. Internal firewalls and NIDS refer to devices that are internal to the TOCs.

A-129. Prior to transmission, the data is encrypted and encapsulated to protect it from prying eyes. Information cannot be viewed, modified or intercepted in a usable form from these encrypted packets. Additionally, the intercepted information does not provide any useable information about the protected hosts on the WIN-T/MSE network. It uses powerful, industry standard encryption algorithms to ensure that data traveling over the TI, the WANs or the TOC LAN cannot be intercepted.

A-130. Transmission security (TRANSEC) is also an important factor that helps secure information across the various networks. Trunk encryption devices, in-line encryption devices, frequency hopping and time division techniques usually secure transmissions. The TRANSEC combined with one or more of the devices listed above are essential to ensure information security (INFOSEC).

Concept

A-131. Network protection is based on a “defense-in-depth” philosophy as illustrated in Figure A-10. The objective of the defense-in-depth is to set up multiple barriers to an outside intruder, a malicious insider, etc. Each barrier combines protection, detection, and reaction features. The defense-in-depth philosophy consists of protection layers building upon each other as defined below:

- **Layer 1.** The first layer of defense is the external digital perimeter composed of COMSEC, firewalls, security guards, and where necessary, physical isolation serving as a barrier to outside networks such as the non-classified internet protocol router network (NIPRNET) as illustrated in Figure A-10. If a hacker penetrates the firewalls and remains undetected by the NIDS on the interfaces from the outside world, layer 2 protection mechanisms remain in place protecting the network.

- **Layer 2**., The internal digital perimeter, consists of firewalls and/or router filtering, serving as barriers between echelons and/or functional communities. Internal barriers may also be accomplished using COMSEC and guards. If a hacker could penetrate the layer 2 Firewalls and remain undetected by the NIDS on the TOC interface, the layer 3 protection would remain.
- **Layer 3**., This a secure local workstation/platform environment, consisting of individual access controls, configuration audit capabilities, C2 protect tools, and procedures. The final protection mechanisms are comprised of C2 protection mechanisms on the hosts.

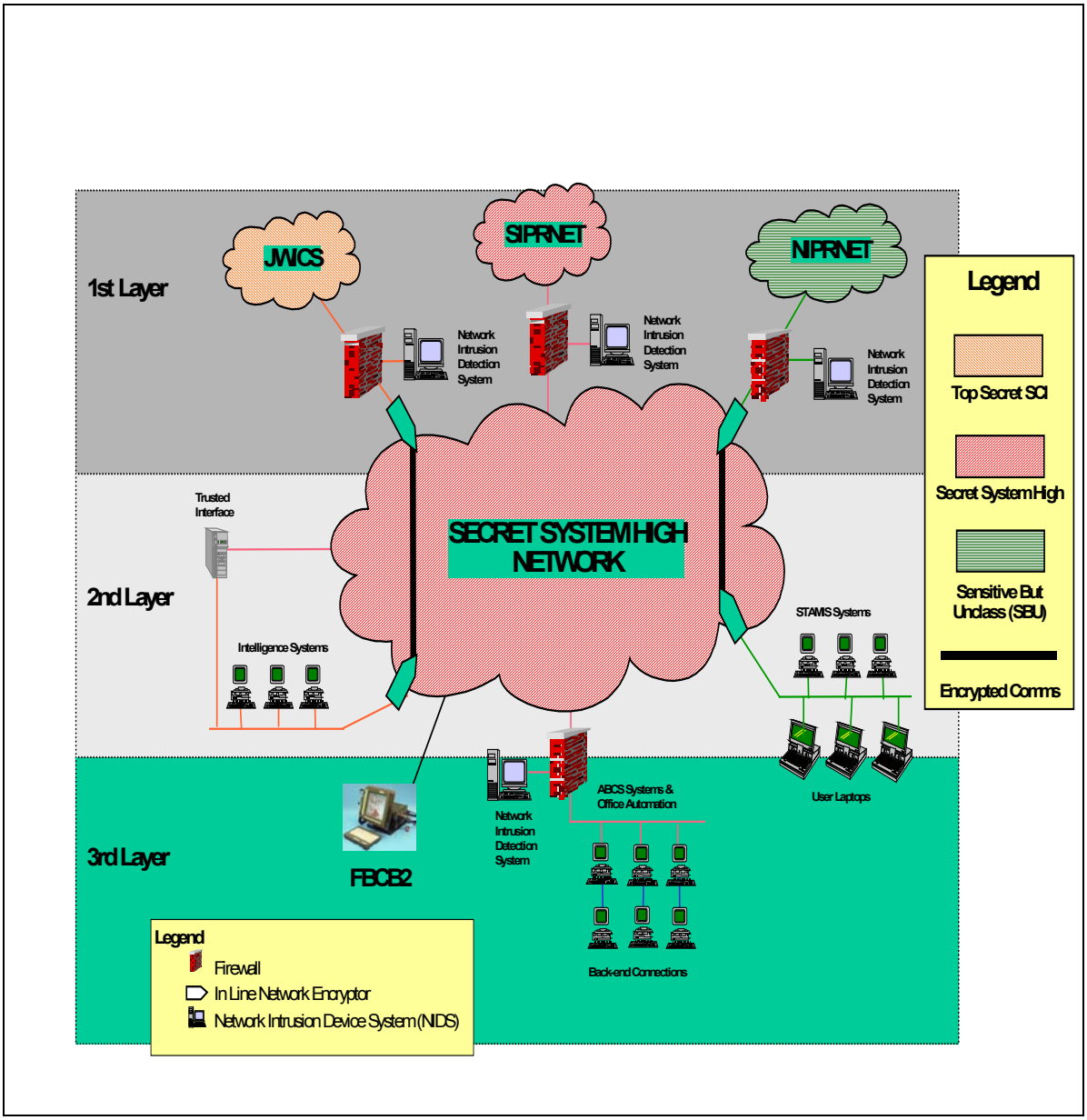

Figure A-10. Concept of Defense-in-Depth Network Protection

A-132. Information systems protection is built into the architecture and design of systems, networks, and overall infrastructure; is implemented concurrent with the implementation of the components of the digitization architecture; and is accessed throughout the development process.

A-133. Criteria for the digitization system architecture balances user performance requirements (typically expressed in terms of connectivity, speed of service or message completion rates) with

security related architecture features such as redundancy, resiliency, and recoverability.

A-134. Information systems protection is designed so that damage is contained and precluded from cascading across the battlefield. The design provides for necessary redundancy and alternate pathways to assure that critical functions can continue in the face of computer attacks. For example, the design provides for alternative routing in the event that selected communications links are jammed or degraded.

Security Services

Firewalls

A-135. The first line of defense within the WIN-T/MSE data networks is protecting access to and from the TI. Without this protection, the door open to the TI is also the door open to the WIN-T/MSE data network. A firewall effectively puts a barrier between the WIN-T/MSE data network and the outside, securing the perimeter and repelling hackers. The firewall acts as a single point of entry where all traffic coming into the WIN-T/MSE data network can be audited, authorized and authenticated. Any suspicious activity based on rules established by the user sets off an alert.

A-136. The axent raptor firewalls used in the external perimeter are software programs that work at the application level. Using a set of application-specific (for example, http, ftp, or H.323) security proxies, the firewall evaluates each attempt to pass data through it for possible security risks. This software is hosted on either an NT workstation or a sun workstation (Solaris 2.6 operation system).

A-137. The axent raptor firewalls will be used at connections between the WIN-T/MSE datanetwork and external networks operating at the same classification level. Fire wall functionality, e.g., router filtering, will be used between WIN-T/MSE data network connections to TOC LANs by configuring the packet filtering rules in the router to block or filter any unwanted protocols and addresses. This same firewall functionality will be used at lower TI connections as well.

A-138. To accommodate the lessons learned and provide the best possible protection for tactical C2, a specific security architecture is being designed and implemented for the FDD information assurance.

Network Intrusion and Detection (NID)

A-139. Protection against intrusion into friendly computer networks through denying unauthorized entry and access into these systems is essential for network protection. The vast percentage of intrusion results from human error. Training and operations security (OPSEC) compliance by system manager, operators, and users are the best measures to combat system compromises.

A-140. An effective method for real-time intrusion detection is to monitor security-related activity occurring on the various systems and devices that make up the network (i.e., routers and switches). The information systems protection lessons learned from the TFXXI AWE and DAWE showed the need for near real time intrusion detection system to identify and react to potential computer attackers. The advantage of real-time activity monitors is that they deploy close to the mission-critical data and applications.

A-141. Specifically, the NID:

- Tracks audit trails from applications, databases, web servers, routers, firewalls, etc. to evaluate system usage over time.
- Monitors critical files for Trojan horses, unauthorized changes, etc. to detect and prevent malicious software from entering into the network.
- Watches TCP and UDP port activity to detect the direction of the network attack.
- Accepts SNMP traps and triggers.
- The NIDS is employed at all external connections to systems (i.e., firewalls).
- The NIDS is employed in TOCs to monitor inter and intra TOC communications.
- Network security management (NSM)/surveillance provides real-time network surveillance and reaction to network intrusion. Robust and resilient infrastructure is designed to "contain" damage from attacks and to be readily reparable in case of attack. The fundamental criteria are that no single attack leads to failure of a critical function, and no single protection mechanism protects critical function or system.
- The NSM security tools are used to identify individual systems vulnerabilities and apply counter-measures before fielding of these systems. One of the most important factors to ensure prevention of intrusion into the automated information systems (AIS) is that all battlespace information systems (BIS) operate in SECRET systems-high mode. Any non-secure system or device connected to or entering any network of secure nature must have an in-line encryption device in use between the network entry point and the entering equipment. This ensures the security of all networks.

Inline Network Encryptor (INE)

A-142. There is one INE for each TOC, vehicle or element with a networked sensitive but unclassified (SBU) workstation for each LAN connection (some have both a hardwire and wireless LAN). The INE will be used to support the transport (i.e., tunneling) of information over the TI at other than the network's system high level.

A-143. System-high use of the MSE packet net today does not require INEs. Users at other security levels will be able to share the transmission media by using INEs for end-to-end cryptographic isolation.

A-144. The present MSE tactical name server/mail transfer agent (TNS/MTA) operates system-high with respect to security, just like the network it serves. Users at other security levels will need some dedicated TNS/MTAs. Though running the same name/mail server software, these would each have an INE, which only accepts connections at its own security level. Unclassified- and secret-level servers might be made co-resident by porting existing TNS/MTA software to a computer with a trusted MLS operating system. There is one INE for each GBS receiver.

Password Control

A-145. Passwords for systems processing classified or unclassified information must be randomly generated with at least an eight-character string using the 36 alphanumeric characters, with at least two of the characters being numeric. The ISSO or designated representative is responsible for overseeing generation, issuance, and control of all passwords. Passwords are issued IAW the following guidelines:

- Users will not have any control over choosing their passwords.
- After generation, password handling and storage are at levels of the most sensitive data contained in the system. Knowledge of individual passwords will be limited to a minimum number of people and not shared. Password issuance is only to users authorized to access the system.
- At the time of password issuance, all users receive a briefing on:
  - Exclusiveness, classification, and uniqueness of each password.
  - Safeguard measures required for classified and unclassified passwords.
  - Prohibitions against disclosure to unauthorized personnel to include personnel assigned to the same project and hold identical clearances.
  - Requirement to inform an ISSO immediately of password disclosure or misuse or other potentially dangerous practices.
  - Issuance of the same password only once. Passwords will be retired when the time limit has expired or the user has transferred to other duties, reassigned, retired, discharged, or otherwise separated from the duties or the function for which the password was required.

Passwords, as unique identifiers of individual authority and privileges, are strictly for use by one user.

- All passwords on classified systems change at last quarterly. Passwords on Non-sensitive and SBU systems change at least semi-annually.
- Passwords need protection against unauthorized observation on terminals and video displays. Each systems operator is responsible for securing operations of their systems. This should prevent unauthorized password observation.

C2 Protect

A-146. Command and control protect (C2 Protect) encompasses those measures taken to maintain effective C2 of our forces by turning to friendly advantage or negating adversary efforts toned information to influence, degrade, or destroy the friendly C2 system. Commanders develop comprehensive protection programs in anticipation of how an adversary will employ elements of attack and intrusion to disrupt the C2 systems and decision-making processes. Listed below are the five principles of IA and protection.

- Gain C2 superiority. This includes functions such as the unimpeded friendly processing of information, accurate development of courses of action, valid decision making, and efficient communications to and from subordinates.
- Remain inside the adversary's decision cycle by denying, influencing, degrading, and/or destroying the adversary's C2, personnel, equipment and systems.
- Reduce the adversary's ability to conduct attack.
- Reduce friendly C2 vulnerabilities using protection measures. For example, hardening information systems with protection devices and techniques to deter attacks and intrusions.
- Reduce friendly interference in our networks and systems throughout all levels of NSM.

Communications Security

A-147. The COMSEC in networks is an absolute must. Specific keys enable encryption of the voice and data passed through transmission devices and computers. The national security agency (NSA) controls most encryption keys or dictates, by regulation, other keys locally generated and distributed. Overall, COMSEC responsibilities rest with the G6/S6/S3.

A-148. Inherent in both the EPLRS and SINCGARS are significant security features. These features include complex low probability of intercept (LPI) transmission techniques, data coding techniques, and data encryption. These security features are augmented with additional specific security techniques to provide system integrity.

Host-Based C2 Protect

A-149. A variety of host-based C2 Protect applications can be found on ABCS and secure UNIX configuration is provided in UNIX configuration guidance for ABCS. Among these are the following:

- The DII COE provides an automated UNIX configuration tool.
- The TCP wrappers are used to authenticate TCP and UDP connections to hosts.
- Security profile inspector is used to identify modifications to system-critical files.
- The SWATCH monitors system audit files for refused connections identified by TCP wrappers, and issues an alert.
- Secure shell provides a strong authentication and secure communication for FTP, TELNET, and others.
- The password checker is used to check selectable passwords to insure they meet revised AR 380-19, Information Systems Security, that requires an 8-character password with 2 numerics.
- McAfee's Virus scan for Solaris provides on-demand protection of PC viruses on UNIX.
- Purge is a non-destructive hard disk (SCSI) declassification software program.

Emergency Procedures

A-150. There are cases requiring drastic procedures to protect networks. The following procedures are carried out only after directed to do so by the commander, or under extreme emergencies. These emergencies are normally covered in a unit's SOP:

- Zeroize COMSEC devices.
- Purge systems.
- Destroy classified systems only when capture is imminent.
- Notify activities as required to enable a proper response.

FBCB2 Perspective - C2 Protect

A-151. The FBCB2 operates at a system high mode, as defined in AR 380-19 and PEO command, control, and communications systems (PEO C3S) security policy; and supports a C2 level of trust, as defined in DOD 5200.28-STD. System high is a mode of operation wherein all users of the FBCB2 computer system possess the required security authorization, but not necessarily a need-to-know, for all data handled by the FBCB2 system. The FBCB2 software supports operation at either of two system (High) sensitivity levels, secret or sensitive but unclassified (SBU). The system sensitivity level controls message marking, message rejection, and screen marking functions.

A-152. In accordance with the principle of “least privilege”, FBCB2 limits the user to only those operational capabilities and data needed to perform the user’s assignment in accordance with the user’s role. When accessing FBCB2, the user is identified by a user group (e.g., the user’s platoon), and a role sensitivity level, which identifies the maximum sensitivity level (SBU or Secret) of data that can be made available to the user. The system sensitivity level is set based on the role sensitivity level of the logged-in user. Further, FBCB2 restricts the user to functionality based on one of four access levels indicating authority/responsibility, pre-assigned to positions in the force structure. This enforces a “role-based” method of access control. Separate security roles are also defined for the security officer (SO), system administrator, and maintainer.

A-153. The FBCB2 requires the user to log into the system prior to granting the user functional access to FBCB2 data. If the users own geographical position data are displayed prior to login, access to FBCB2 functionality and data will be granted after entry of the user group identity. The user must then enter a valid password that matches to this identity and the user’s role sensitivity level, and acknowledge an AR 380-19 compliant computer log-on banner notice. This is a text notice warning to the user that appropriate authorization is required to enter the system and that the user is subject to monitoring.

Access Control

A-154. The FBCB2 software provides an operational user the capability to initiate an emergency disable request in the event of an overrun and anticipated capture of an FBCB2-equipped vehicle/TOC. In response to such a request, FBCB2 overwrites the hard disk and resets the router to its factory default configuration.

A-155. The FBCB2 rejects incoming C2 JVMF messages when the message sensitivity level of the incoming C2 JVMF message, as indicated in the JVMF message header security classification field, exceeds the system sensitivity level.

A-156. When connected directly to the router, in the fielded configuration, the INC router authenticates the FBCB2 host via the challenge handshake authentication protocol (CHAP). The FBCB2 responds to authentication requests from the INC router, at router initialization when the PPP link is established, and periodically thereafter during router operation, by supplying the router authentication password in accordance with the CHAP. The INC router will not communicate to an FBCB2 host that fails this authentication. The FBCB2 configures the INC router operational data by affecting SNMP write operations (i.e., sets) on the INC MIB. The FBCB2 supplies the INC configuration password to the INC prior to the configuration process. The INC router grants access to the FBCB2 host for router configuration based on validity of the

password. The INC router will not perform the configuration processes if the FBCB2 host fails authentication. For each requested set of INC MIB data, FBCB2 will supply an SNMP community name. The INC router will not perform the SNMP set operation if the community name is invalid.

A-157. The FBCB2 restricts functional users from direct access to the command line of the operating system, from directly executing operating system commands, and from escaping to the operating system through keyboard action.

Security Status Reporting

A-158. The FBCB2 audits a refined set of security critical event exceptions. For example, the event of a user's failure to enter a correct password after successive retry, will be audited. Audited events are not saved locally. They are forwarded via the security JVMF message to FBCB2 hosts within the lower TI, actively running the security officer (SO) role, where they are collected for review and disposition by the SO(s). Effective routing of audit event messages to hosts actively running the SO role, are achieved through the use of designated SO multicast groups. Each SO is provided the capability to log security events, and to archive the log. Audited events include the following data: type of event, date and time the event was detected, role and URN of the host logged in (if any) at the time of the event, geographic location of the event (if available), and success or failure (if applicable) of the event.

Labels

A-159. The FBCB2 marks all screens to reflect the system sensitivity level. The TOC LAN configuration could include a printer accessible to FBCB2. The FBCB2 marks printed output to reflect the system sensitivity level, in accordance with AR 380-5, Department of the Army Information Security Program. The FBCB2 marks C2 messages generated automatically, or created manually by the user, not to exceed the system sensitivity level. The FBCB2 software automatically fills the security classification field of the message header per MIL-STD-2045-47001B. The FBCB2 permits the user to override the default message sensitivity level, of manually created messages, not to exceed the system sensitivity level.

Password Management

A-160. Password management is a set of services for the SO to manage passwords. These services include generation of AR 380-19 compliant passwords, assigning the passwords to user groups, and loading them in sets on individual target FBCB2 computers. Services are also provided for the SO to display and update the

status of password assignment and loading. In accordance with signal operating instructions (SOI) procedure, the SO records the passwords and identifiers off-line.

Purge

A-161. The FBCB2 supports, if available, government furnished equipment (GFE) provided off-line purge capability. Purging is performed on magnetic hard disks by overwriting all locations with a character, its complement, then with a random character.

Anti-Viral Protection

A-162. The FBCB2 incorporates a GFE provided method of malicious code detection.